RPAガバナンス構築のためのガイドライン

2019年10月

PwCあらた有限責任監査法人
UiPath株式会社

はじめに

労働人口不足や働き方改革などを背景に、労働生産性の向上があらゆる組織において喫緊の課題となっています。その解決手段の一つとして、近年多くの企業がロボティック・プロセス・オートメーション（Robotic Process Automation。以下、RPA）の導入を進めており、高い効果が期待できる業務へ適用することを目指しています。適切なRPAガバナンスを構築し、そのような業務へRPAの導入を成功させ、経営課題解決へ前進している企業もあります。一方で、十分な管理体制や管理ルールを定めないままRPAを導入したことにより、管理者不明の「野良ロボ」問題やロボット専用IDの不正利用などといったリスクが顕在化している企業もあります。これらのリスクを懸念して導入が停滞するケースや、実際にリスクが顕在化して導入目標を達成できないケースも出てきており、このままでは、労働人口不足や働き方改革にかかわる経営課題や社会課題の解決に向けた取り組みが阻害されてしまうおそれがあります。このため、多くの企業で、RPAを安全・安心に導入・利用していくための仕組みであるRPAガバナンスの構築が急務となっており、参考となる基準やガイドラインが必要とされています。

そこで今回、RPAを安心して導入・利用するに当たり、どのような体制であるべきか、どのような観点で管理を行っていくべきかなど、RPAガバナンスの構築、運用におけるポイントや参考となる考え方をガイドラインとしてまとめました。

本ガイドラインは、特定のRPA製品を対象としているわけではなく、どのRPA製品においても適用できる汎用（はんよう）的なものとなっています。よって既にRPAを導入している企業、またこれから導入していく企業等、多くの方が本ガイドラインをご参照いただくことを想定しています。PwCあらた有限責任監査法人およびUiPath株式会社は、本ガイドラインの策定と公開に加え、セミナーや具体的なRPAガバナンス構築に関するサービス提供等を通じて、RPAガバナンスの浸透、普及に向けた啓発活動を行います。これらの活動を通じて、RPAの安全・安心な導入と利用普及により、人や労働にかかわる経営課題を解決、ひいては労働人口の減少といった日本の社会問題の解決にお役に立てればと考えております。

PwCあらた有限責任監査法人
パートナー
宮村 和谷

UiPath株式会社
代表取締役CEO
長谷川 康一

目次

第1章　本ガイドラインの位置付け

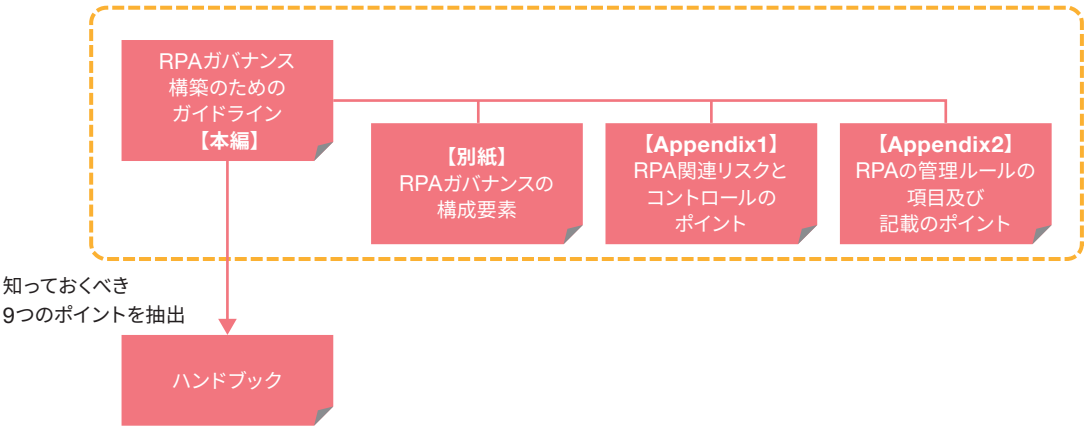
1. 目的

RPAガバナンス構築のためのガイドライン（以下、本ガイドライン）は、組織が業務に対してRPAを安心して導入・利用するために必要となる戦略、体制、管理ルールといったガバナンス、ガバナンスを構築する際のポイントや運用、モニタリング、改善等の参考となる考え方を説明することを目的としている。

2. 本ガイドラインの位置付け

本ガイドラインは、RPAガバナンスの構成の全体像や構築方法、運用等を網羅的に記載したものである。なお、参考資料として、本書の知っておくべきポイントを抽出した内容や対応事例を掲載している「RPAガバナンスハンドブック」があるため、必要に応じて参照いただきたい。

図1：本ガイドラインの位置付け



3. 対象

本ガイドラインは以下のとおり、特定の業界や組織、利用形態、導入状況、製品を対象としたものではない。RPAにかかわるあらゆる状況、状態でも利用可能なものとしている。

- あらゆる業界・組織・利用形態を対象にしている
  特定の業界、組織や利用形態に特化した内容ではなく、広範囲の業務やさまざまな利用形態でのRPAガバナンス導入・利用において参考となるよう考慮している。
- あらゆるRPA導入状況を対象にしている
  これからRPAを導入する組織だけでなく、既にRPA導入を進めている組織等も対象としているため、パイロット導入期にある組織や本格導入期においてより高度な利用を目指す組織も対象としている。
- あらゆるRPA製品を対象としている
  RPAガバナンスにかかわる基本的な考え方を述べたものであり、特定の製品に特化した内容ではなく、一般的なRPA製品を想定した内容となっている。そのため、さまざまなRPA製品を利用する組織において参考となるよう考慮している。

4. 用語の定義

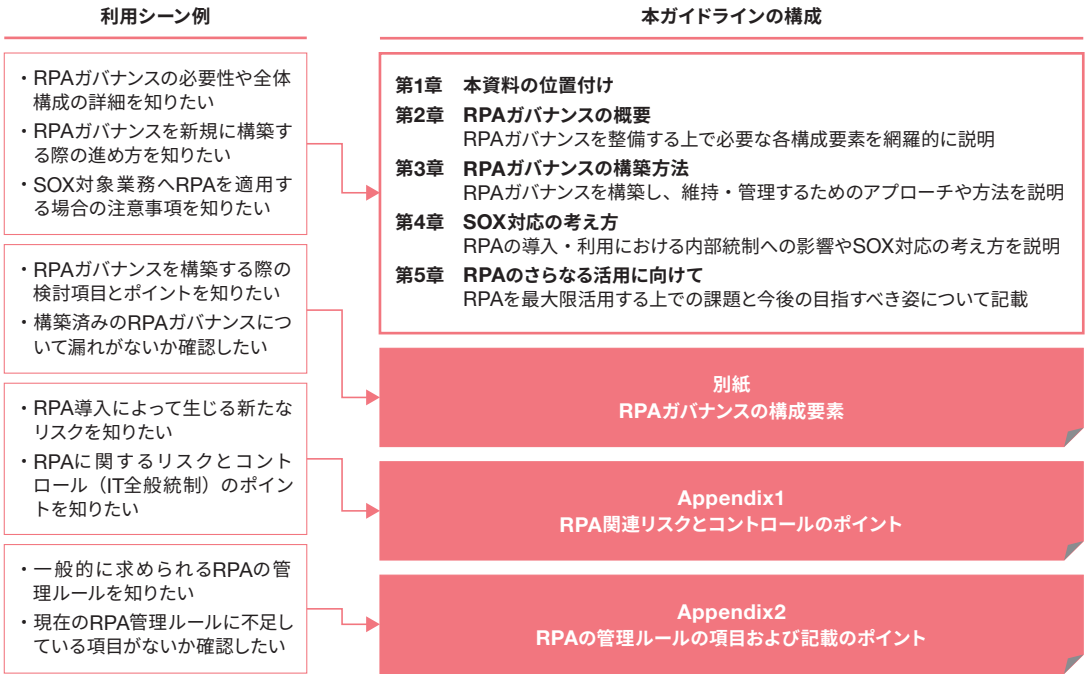
本ガイドラインに記載されている用語の定義を以下に記す。

用語	説明
RPA	Robotic Process Automationの略であり、人がパソコン端末等を使用して行っていた業務プロセスの全てまたは一部を、ソフトウエアロボットを使用して自動化する仕組みのこと。
RPAツール	ソフトウエアロボットの作成や実行を行うためのソフトウエア製品のこと。
RPAシステム	RPAを利用するために必要な RPAツール、ロボット端末、ロボット管理サーバー等を含めたシステム全体のこと。
ロボット	RPAツールにて作成されたソフトウエアロボットのこと。パソコン端末で人が行っている業務処理を、設計されたプログラムに従って代替処理する。
ロボット端末	RPAツールをインストールし、ロボットの開発や実行を行うための端末のこと。パソコン端末の場合や仮想デスクトップの場合がある。
ロボット管理サーバー	サーバー型のRPAシステムにおいて、ロボットのリソース管理、スケジュール管理、実行監視、ログ管理等を行うための管理サーバーのこと。
サーバー型	ロボット管理サーバーが、実行用シナリオ端末に対し、シナリオの配信や実行、実行状況の監視、管理情報の提供などを行うRPAシステムの形態のこと。
デスクトップ型	実行用ロボット端末自体にロボットの実行ファイルを保存し、単独で実行するRPAシステムの形態のこと。そのようなRPAツールや利用形態のことを Robotic Desktop Automation（RDA）と呼ぶこともあるが、本書ではRDAも含めて広義にRPAと呼ぶ。
ロボット専用ID	RPAの適用により自動化の対象となるシステムのIDをロボット専用に発行したもの。

5. 本ガイドラインの構成と想定される利用方法

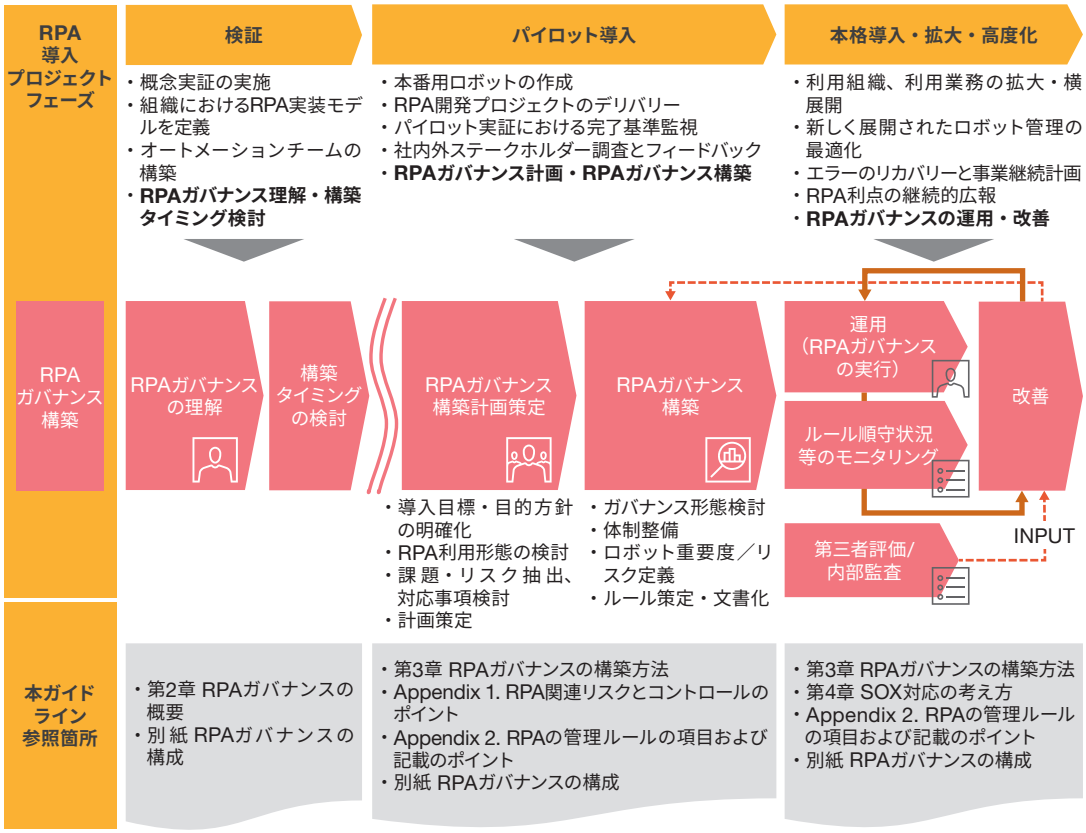
本ガイドラインは、第1～5章と別紙、Appendix1、2にて構成されている。また、RPAガバナンスの構築状況ごとに応じて重点的に参照すべき箇所が異なる。利用シーンに応じた本ガイドラインの利用方法については図2を参照していただきたい。

図2：本ガイドラインの構成と利用シーン（例）



下記の図3は新規にRPAガバナンスを構築する場合の例である。主に導入前の検証時点、パイロット導入時点、本格導入・拡大・高度化の3つのフェーズに分けて、それぞれのフェーズに応じて特に参照すべき箇所を記載している。よって各フェーズで何を行うべきか知りたい場合は、以下を参照していただきたい。

図3：RPAガバナンス構築状況に応じた本ガイドラインの利用方法（例）



6. 関連する公知の基準・ガイドライン

RPAは、IT（情報技術）の一種であり、ITガバナンスやシステムリスク管理に関する公知の基準やガイドラインの考慮が必要となることもある。本ガイドラインでは、第2章「5.構成要素」の項目を検討するにあたり、「COBIT2019（ISACA）」と「主要行等向けの総合的な監督指針（金融庁）」を参考とした。各項目との関連付けを別紙「RPAガバナンスの構成要素」に記載しているので、必要に応じ参照いただきたい。

なお業種や導入拠点（海外等）によって、これら以外の基準やガイドラインが求められることもあるため、注意する必要がある。

7. 免責事項

- 本ガイドラインは、最適なRPAガバナンスの構築を保証するものではなく、利用者の自己の責任において参考として利用することを前提としている。
- 本ガイドラインに含まれる情報に基づき、RPAガバナンスの構築や見直し、評価を行ったことにより被った損失や損害について、PwCあらた有限責任監査法人およびUiPath株式会社は、いかなる責任や義務を負わない。

8. 知的財産権

- 本ガイドラインに関する著作権を含む一切の権利は、PwCあらた有限責任監査法人およびUiPath株式会社（以下「作成者」と総称する）に帰属しており、著作権法その他の法令により保護されている。本ガイドラインの利用にあたっては著作権法その他の法令および作成者の定める事項（本項に記載の事項を含む）を順守すること。
- 本ガイドラインに記載されている情報については、非営利目的且つ利用者の組織内での使用に限り、使用及び複製（ファイルコピー、ダウンロード、プリントアウト、その他の方法含む）することを許諾する。しかし、その複製物を第三者へ譲渡または移転することは、作成者の許諾がない限り、いかなる場合および方法においても禁止とする。
- 作成者による許諾なく、上記において明示的に許諾された範囲を超えて、本ガイドラインを複製、改変、転載、加工し、または営利目的で利用することは禁止とする。
- 本ガイドラインに記載されている全ての商標、ロゴマークおよびサービスマークは、PwCあらた有限責任監査法人またはUiPath株式会社 がライセンスを有し、正当な権限に基づき使用する商標である。権利者の許諾を得ることなくこれらを無断で使用することは禁止する。

第2章　RPAガバナンスの概要

本章では、RPAガバナンスの全体像とガバナンスを構成する構成要素について説明する。RPAガバナンスの構築方法は第3章にて説明する。

1. RPAガバナンスの必要性

デジタルレイバー技術の一つであるRPAの導入事例は、さまざまなメディアで取り上げられ、世間をにぎわせている。RPAの特徴やメリットについては、いろいろな所で紹介されているため割愛するが、上手に導入・活用できれば、ルーティンワークに要する時間の削減などの効果が得られる。しかしながら、RPAはただ単に導入すれば良いものではない。例えば、RPAの利用を本格化させようとしている企業からは、以下のような課題が聞かれる。

RPA導入プロジェクトでよく聞く課題（例）

分類	よく聞く課題（例）
RPA導入プロジェクト全体	・RPAの導入目標や目的が不明確となり、短期的な目標・目的達成のために導入が進み、結果としてRPA導入によって本来解決すべき課題が解決されない。 ・リスクを考慮してRPA適用業務を制限しているが、自動化の範囲が限定されるため、当初計画していた効率化が達成できない。 ・明確な基準がないままRPAの導入が拡大しており、組織としてRPA導入により生じるリスクを適切に把握できていない。
ロボットの開発	・開発時の開発ルールやレビュー等が不十分であるため、異常発生時の処理の考慮が十分でないロボットがリリースされ、ロボットの品質が低下し、頻繁にロボットが止まってしまうことで結果として業務に影響を及ぼす。 ・開発した本人しかロボットの変更や障害対応ができないなど、保守性のないロボットが増え、ロボットの保守コストが増大化している。 ・チェックプロセス等がないため、本番環境でのロボットテスト後、本番データの更新を戻し忘れた。 ・ロボットが操作する本番システムへのアクセス権を開発者が保有しておらず、テストが実施できない。
ロボットの運用	・ロボット専用IDの発行が禁止されている。 ・ID・パスワードの保存場所、権限設定、パスワード変更等、どのようにロボット専用IDを管理すればいいか分からない。 ・利用されているロボット端末やロボット専用IDの管理が不十分なため、不正に端末やロボットが利用されるなど、セキュリティ上の問題が顕在化する。 ・ロボットが停止すると業務に影響を与えるが、十分な対応体制、障害対応手順、インシデント管理方法が整備されていない。 ・操作する情報システムの変更により、複数のロボットが同時に動かなくなった。
その他	・SOX対応業務におけるロボットによる処理の組み込みが不十分なため、会計データや処理の信頼性が損なわれ、誤った会計処理をするおそれがある。また、会計監査人による指摘を受ける。 ・SOX対象業務にRPAを適用する場合の影響や考慮事項が分からない。 ・SOX対象業務の自動化が禁止されており、自動化が思うように進まない。

一部の組織では、実際にこのような課題が顕在化したために、RPA導入計画の見直し、当初企図していた課題解決への取り組みが停滞してしまうケースも見受けられる。では、このような事態を避け、RPA導入における目的・目標を達成するためにはどのような仕組みがあればいいのか。そこで必要となるものが、「RPAガバナンス」である。

2. RPAガバナンスの概念 － ITガバナンスや情報セキュリティガバナンス等、既存の仕組みとの関係

これまで各企業は、ITガバナンスやシステムリスク管理態勢、情報セキュリティガバナンス、J-SOX[1]やUS-SOX[2]におけるIT全般統制等の構築を行ってきた。これら取り組みを行う中でRPAが新たに登場し、その管理をどうすべきか検討することとなった。RPAは、ただそれだけを見ると非常にシンプルなものであるが、以下のとおり管理を難しくさせる要因がある。なお、本ガイドラインでは、J-SOXとUS-SOXを総称する場合、「SOX」と表記する。

①まざまな解釈の存在 － マクロの延長、人の代わり、システムと同等

RPAの話をしていると、人によってロボットの解釈が異なる。「マクロの延長」という者もいれば、「人の代わり」という者、「システムと同等」という者もいる。同じ会社や部署の中でも全く異なる解釈をしている場合も多い。

例えば、「マクロの延長」と解釈している場合は、表計算ソフトでの集計等、単に同じような利用形態をしているだけであり、ロボットによるシステムへのデータ入力等、プロセスの自動化によるリスクまで認識できていない、またはそのようなリスクに目をつぶっている場合がある。「人の代わり」と解釈している場合は、「ロボットもミスをする」という前提でロボットの処理結果を人がチェックするようにしているが、そのチェックが過剰となり、折角の自動化による効率化機会を逃している場合もある。また「人の代わり」であるため、ロボット専用にIDを発行する場合もあるが、当該IDの管理が不十分で、ID・パスワードが漏えいするリスクがある。「システムと同等」と解釈している場合は、あらゆるロボットに対し通常のシステム開発・運用と同等レベルの管理を求め、結果として工数が増加し費用対効果を悪化させたり、場合によっては過度な管理を敬遠され、RPA導入自体が進まなくなるようなリスクがある。

これらはRPA固有のリスクとなるものであり、既存のITやシステムの管理の仕組みの中ではカバーできない可能性がある。

図4：ロボットの位置付け

1　J-SOXとは、金融商品取引法の財務報告に係る内部統制報告制度の呼称である。

2　US-SOXとは、米国の企業改革法（サーベンス・オクスレー法）第302条、404条に基づく内部統制報告・監査制度である。ニューヨーク証券取引所への上場等、SEC登録企業はUS-SOXが適用される。

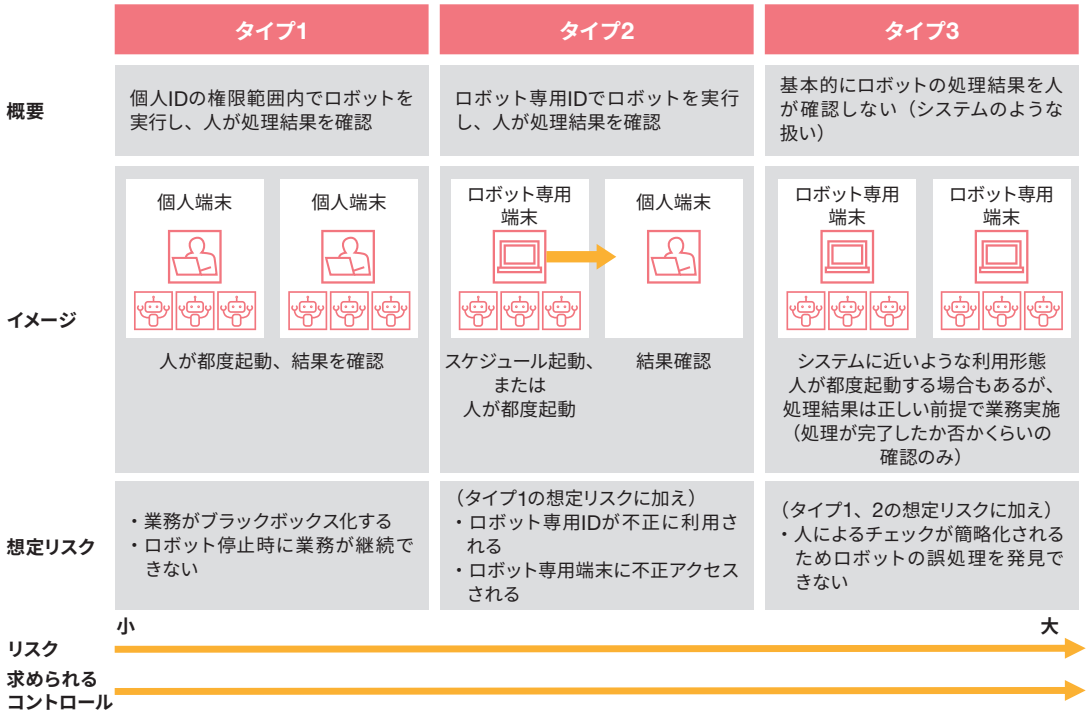
②利用形態によって異なるリスクと求められるコントロール

上記①とも関係するが、一言でRPAといっても利用形態はさまざまであり、それによってリスクと求められるコントロールが異なるというのも、RPAの管理等を難しくする要因となっている。

例えば、個人IDの範囲内で開発・利用する場合、あくまで個人IDの範囲内であるため、システムへの誤入力等、責任は明確である。また業務プロセスに有効な内部統制が整備されていれば、そのような誤入力は予防・発見できるであろう。一方で、ロボット専用にIDを発行し、当該IDでロボットが各システムにアクセスする場合、もしもロボット専用IDの管理が不十分であるならば、管理者がロボット専用IDで経費入力し、自身の個人IDで承認するなど、ロボット専用IDの不正利用リスクも高まるであろう。また、さらなる効果を求め、人の介在を極力減らしたシステムと同等の使い方を行う場合、人によるチェックを割愛し、ロボットの処理結果に依存して業務を行えば高い効果を得られるが、誤処理を発見することは困難になることも予想される。さらに、元々の業務を行っていた人も減り、ロボットが停止した場合、人が手作業で業務を行いリカバリーさせることは難しくなるであろう。

このように、利用形態によって異なるリスクがあり、また求められるコントロールが変わる。このことが、RPAの管理をより一層難しくさせている。

図5：RPA利用形態のイメージ



前述で述べたとおり、RPAの管理は難しいということが分かる。それゆえ、ITガバナンスやセキュリティガバナンスといったこれまでの仕組みとは別に、「RPAガバナンス」という仕組みが必要となっている。

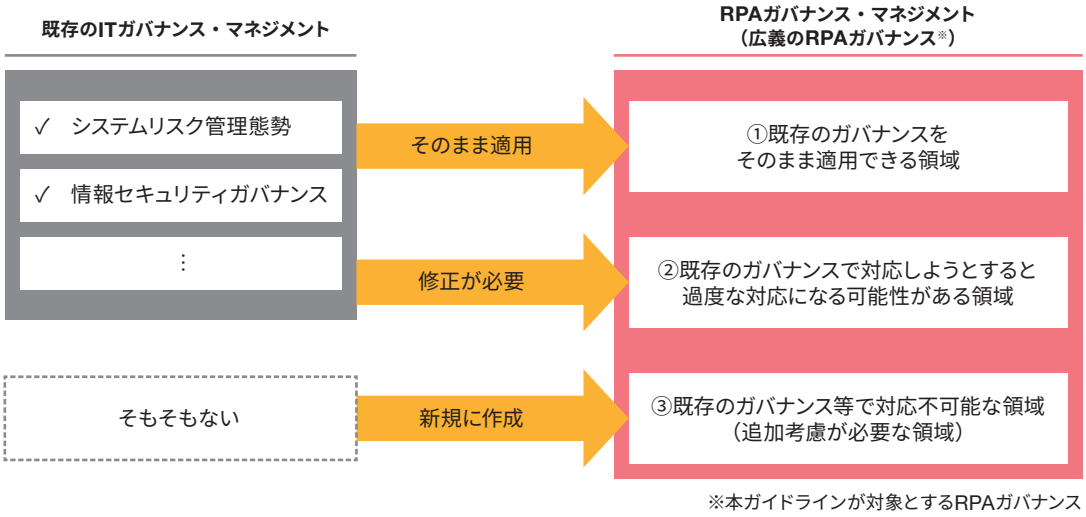
RPAはこれまで企業が構築してきたITガバナンスやシステムリスク管理態勢、情報セキュリティガバナンス、IT全般統制等ではカバーできない領域、無理にカバーするとRPAのメリットを阻害するような領域がある。よって、RPAガバナンスの制定に当たっては既存のガバナンスとの関係性を以下の①～③観点で整理する必要がある。

①既存のガバナンスをそのまま適用できる領域

②既存のガバナンスで対応しようとすると過度な対応になる可能性がある領域

③既存のガバナンス等で対応不可能な領域（追加考慮が必要な領域）

図6：RPAガバナンスと既存のガバナンスとの関係



※本ガイドラインが対象とするRPAガバナンス

3. RPAガバナンスの全体像

RPAガバナンスとは、RPAの導入目標・目的を安心して達成していくための仕組みである。

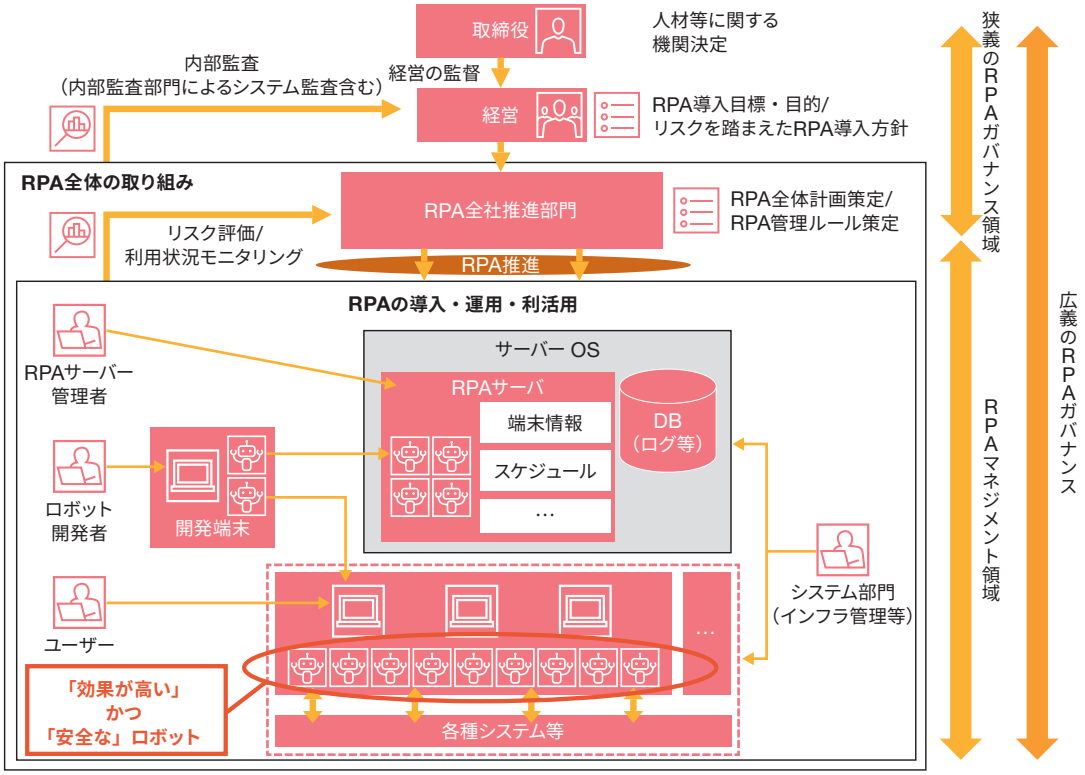
RPAは、その利便性や開発容易性から、ユーザー主導で導入が進むこともある。その場合、ITに詳しい担当者が確保できず、十分な管理がされない状態でRPAの導入が進むことも考えられ、本章「1.RPAガバナンスの必要性」の課題例が現実となる可能性がある。

このような事態にならないよう、会社として満たすべき管理水準の策定や、管理水準を満たすための体制の整備といった“会社として一定の管理水準を満たしていくための仕組み”として、RPAガバナンスを構築する必要がある。その際、管理ルールの策定や推進部門の整備だけでは不十分である。 方針やモニタリング等の「狭義のRPAガバナンス」に加え、体制やルール等の「RPAマネジメント」にも取り組むことが望まれる。

なお、本ガイドラインでは、「狭義のRPAガバナンス」に「RPAマネジメント」を包括した、広義の「RPAガバナンス」としている。

RPAガバナンスを適切に構築・運用することで、RPAのメリットを享受しつつ、安全に導入・利用が進めば、RPA導入目標・目的を達成し、結果として人や労働にかかわる重要な経営課題の解決につながることが期待できる。

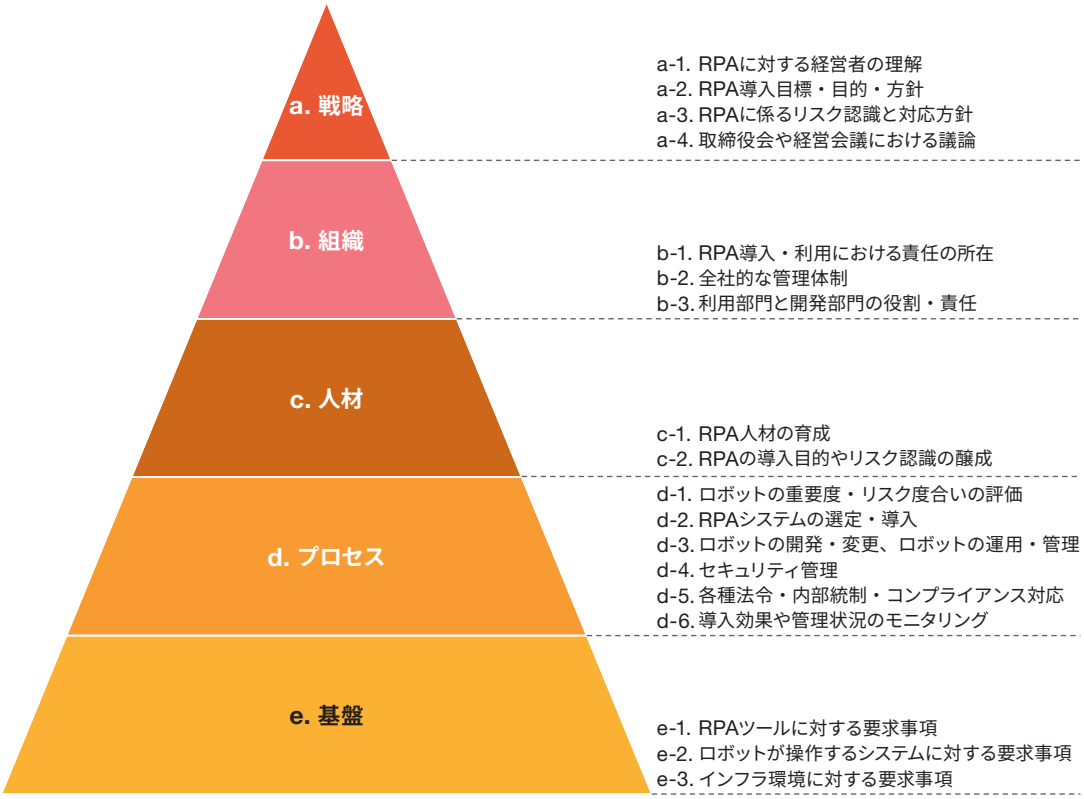
図7：RPAガバナンス全体像のイメージ



4. RPAガバナンスの構成要素

前述のとおり、RPAガバナンスは“会社として一定の管理水準を満たすための仕組み”である。この仕組みは、「戦略」「組織」「人材」「プロセス」「基盤」の5つの領域で構成される。これらは、特定の領域に偏っていたり、欠けていたりする場合、RPAガバナンスの有効性は限定的なものになる可能性がある。全ての構成要素が必須というわけではないが、一度それぞれを確認し、自社における過不足等を確認されることが望まれる。

図8：RPAガバナンスの構成



5. 構成要素の説明

戦略、組織、人材、プロセス、基盤の5つの構成要素について、概要とポイントを記す。詳細な説明は別紙「RPAガバナンスの構成」を参照していただきたい。

a. 戦略

項	構成要素	概要	ポイント
a-1	RPAに対する経営者の理解	経営者もRPAの特徴、活用することの価値、経営へのインパクト等を理解する。	(1) RPA等といったデジタルテクノロジーについて、経営者自身も積極的に理解しようとしていること。 (2) 時間削減といった短期的な効果だけでなく、高付加価値業務へのシフトや採用難等といった人材や労働にかかわる経営課題解決のツールになると理解していること。 (3) 企業経営のプラットフォームとなるのか、単なるデジタルツールの一つなのか、RPAの位置づけを検討すること。 (4) RPAを導入しない場合の中長期的な影響、リスクについても理解していること。
a-2	RPA導入目標・目的・方針	企業ミッションを踏まえ、RPAをどのような効果を得るために導入し、活用するかの目的を明確化する。	(1) RPA導入によって解決すべき経営課題や、達成すべき短期的および中長期的な目標が明確化されていること。 (2) 会社としての明確な導入方針が定められていること。
a-3	RPAにかかわるリスク認識と対応方針	RPA導入により生じるリスクを認識し、そのリスクに対応するため、RPAガバナンスを整備する方針を明確化する。	(1) RPA導入によって生じるリスクを認識すること。 (2) RPA導入・利用におけるリスク対応方針や、経営者が従業員に求める管理方針・ルール等が定められていること。ただし、認識したリスクに対し過度にならないこと。
a-4	取締役会や経営会議における議論	RPAの導入方針やリスク対応方針について、経営層で議論し、合意する。	(1) 経営会議や取締役会等で、RPA導入方針やそれに伴うリスク対応方針が議論されていること。 (2) 経営会議や取締役会等で、RPA導入方針、RPAガバナンス整備状況、RPA導入による効果等のステークホルダーへの公開が議論されていること。

b. 組織

項	構成要素	概要	ポイント
b-1	RPA導入・利用における責任の所在	RPAを導入することに対する経営者の役割・責任やRPAガバナンスを機能させる責任を負う担当役員の設置を明確化する。	(1) RPA導入・利用における経営者の役割・責任が明確化されていること。 (2) RPAガバナンスを機能させる責任を負う担当役員が選任されており、またその役割が明確化されていること。
b-2	全社的な管理体制	RPAガバナンスを機能させるために必要となる全社的な体制とその役割・責任を明確化する。	(1) 各組織形態（集権型・分散型・連邦型）のメリット・デメリットを理解し、組織に応じた組織形態を組成し、必要となる推進・管理部門を設置すること。 (2) 推進・管理部門には、ロボット利用状況の把握やセキュリティレビュー等、会社として一定レベルの管理水準を担保するための機能を持たせること。または推進・管理部門を設置しなくとも、各部門で不適切なロボットの利用がなされないための仕組みを整備すること。
b-3	利用部門と開発部門の役割・責任	RPAを導入して利用する部門や開発部門の役割・責任について明確化する。	(1) RPAを導入して利用する部門やロボットを運用する部門の役割と責任を明確化すること。 (2) ロボットを開発する部門の役割と責任を明確化すること。 (3) ロボットの開発者、利用者、運用者の分離、ロボットの実行可能権限とその作業の承認権限の分離等、職務分離が検討されていること。

c. 人材

項	構成要素	概要	ポイント
c-1	RPA人材の育成	RPAガバナンスを機能させるために必要な人員やロボットの開発・運用に必要な人材を確保するための育成や採用方針、外部委託先の活用方針を明確化する。	(1) RPAの概念やRPA導入目的・目標を理解させる取り組みが行われていること。 (2) ロボットの開発や運用に必要な人的リソース（質・量）が洗い出され、その育成や採用、外部委託先の選定等が行われていること。 (3) ロボット開発や運用の内製化を目指す場合、必要となるスキルが明確化され、内製化に向けた開発スキルの教育計画やロボット開発ナレッジを蓄積する仕組みが整備されていること。
c-2	RPAの導入目的やリスク認識の醸成	RPA導入の目的や導入により生じるリスク、それに対応するための管理ルール等を認識させる。	(1) 全ての従業員またはロボットが行う業務にかかわる従業員に対し、RPAの導入方針や管理ルールに関する教育を実施していること。 (2) 従業員へ伝えるRPAの導入方針には、ロボットによる自動化、効率化、コスト削減だけでなく、RPAの活用によりビジネス、組織、従業員、プロセスをどのように変革させていくかの戦略や目的を含めること。

d. プロセス

項	構成要素	概要	ポイント
d-1	ロボットの重要度・リスク度合いの評価	どのようなロボットのリスクが高いかを定義し、管理を強化すべきロボットを特定する手続きを明確化する。	(1) ロボットの重要度やリスク度合いの定義やその判断基準が明確化されていること。 (2) 重要度やリスク度合いに応じたロボットの管理水準・管理ルールが明確化されていること。 (3) ロボットの重要度やリスク度合いを評価する手続きが明確化されていること。
d-2	RPAシステムの選定・導入	RPAを適用する業務領域に求められるロボットの信頼性や管理機能などから、RPAツールや基盤を選定し、導入するプロセスを明確化する。	(1) 新たな業務領域へのRPAの適用について、検討や承認プロセスが定められていること。 (2) RPA適用が承認された業務領域について、その重要度や取り扱うアプリケーション、将来的な拡張予定などに応じて、ロボットに求める信頼性、性能、管理機能などの要件を明確化し、RPAツールや基盤を選定し、導入する手続きが定められていること。 (3) 新たなRPAシステムを導入する場合は、ロボット管理サーバーやロボット端末などの運用、保守の管理体制や手順を定めるプロセスとして明確化すること。
d-3	ロボットの開発・変更	ロボットを企画する際の考慮事項、開発標準の適用、整備すべきドキュメントなど、ロボットを開発する際に順守すべき事項やロボットリリース時のテスト・承認プロセスを明確化する。	(1) 業務標準化等も含めた要件検討や開発の優先順位付けなど、ロボットを企画する際の手続きが明確化されていること。 (2) 開発標準などのロボット作成時に守るべきルールやリリースまでに整備すべきドキュメントなど、ロボットを開発する際に順守すべき事項が明確化されていること。 (3) エラー処理のテストの実施、RPA利用部門も参画したテストの実施、テスト環境でのテストの場合は本番環境との違いの考慮、本番環境でのテストの場合は本番システムへの影響の考慮など、ロボットをテストする際のチェック項目や留意事項が明確化されていること。 (4) ロボットをリリースする際の承認者や承認時の確認項目などが明確化されていること。 (5) リリース済みのロボットを修正する場合の役割や手続きが明確化されていること。
d-4	ロボットの運用・管理	ロボットを安全かつ安定的に稼働させるために、ロボットの運用・管理プロセスを明確化する。	(1) ロボットの運用にかかわる定例、非定例のオペレーションを明確化し、その手続きを定めること。 (2) ロボットが停止するリスクを低減するための予防的な対策を講じること。 (3) ロボットの処理で異常や遅延が発生した際に、自動的に通報される仕組みまたは人が検知して連絡する手続きを定めること。 (4) 再発が想定されるロボットの処理の異常や遅延について、原因分析や恒久対応を行う手続きを定めること。 (5) ロボットが利用できなくなることを想定したコンティンジェンシープランが策定されていること。 (6) ロボット端末、RPAツール、ロボットなどRPAにかかわる構成情報が管理されていること。

項	構成要素	概要	ポイント
d-5	セキュリティ管理	ロボットやロボットが取り扱うIDやデータを内部不正やサイバー攻撃から守るためのセキュリティ管理プロセスを明確化する。	(1) 内部不正やサイバー攻撃によるセキュリティリスクに応じて、RPAに対して求めるセキュリティ管理要件やセキュリティ対策を検討・実装する手続きを明確化すること。 (2) ロボットの改ざんやロボットの不正実行などを防止するため、ロボットへのアクセスは必要最小限な者に限定するための手続きを明確化すること。 (3) 情報システムなどにアクセスするためのロボットが使用するIDやパスワードは、管理者を定め、不正に使用できないように管理する手続きを明確化すること。 (4) ロボットが取り扱うデータに対するアクセス制御や管理手続きを明確化すること。
d-6	各種法令・内部統制・コンプライアンス対応	RPAを適用する業務が各種法令・内部統制・コンプライアンスに該当するか否かを明確化し、ロボットで行う処理がそれらに対応するよう設計・運用するプロセスを明確化する。	(1) 各種法令、内部統制、コンプライアンスなどに影響を及ぼすロボットかどうかの基準や判断する手続きを明確化すること。 (2) 各種法令、内部統制、コンプライアンスなどに影響を及ぼす可能性のあるロボットの利用を許可する場合、RPAの管理体制や管理ルールはそのリスクを踏まえたものとすること。
d-7	導入効果や管理状況のモニタリング	RPA導入による効果やリスクへの対応状況、ロボットの管理状況をモニタリングするためのプロセスを明確化する。	(1) RPA導入目標（KPI）とその達成状況をモニタリングする仕組みが整備されていること。 (2) 各RPA利用部門でのロボットの導入状況や、各ロボットの重要度・リスク度合いを定期的に確認する仕組みが整備されていること。 (3) 各RPA利用部門に対して、ロボットの開発・運用における管理ルールの順守状況を定期的に評価し、モニタリングする仕組みが整備されていること。 (4) 全社的なRPAガバナンスの状況を内部監査や外部監査で評価し、必要に応じてRPAガバナンスの見直しを行っていること。

e. 基盤

項	構成要素	概要	ポイント
e-1	RPAツールに対する要求事項	利用するRPAツールについて、どのような要件が必要かを検討し、RPAツールを選定する。	(1) さまざまなアプリケーションやテクノロジーとの親和性が高いこと。 (2) ロボット管理機能や異常時の通報機能、ログの出力機能など、ロボットの実行や管理を支援する機能が実装されているまたは拡張可能なこと。 (3) RPAツールの脆弱（ぜいじゃく）性情報やセキュリティパッチが定期的に提供されること。
e-2	ロボットが操作するシステムに対する要求事項	ロボットが操作する社内または社外のシステムについて、どのような要件が必要かを検討し、ロボット操作対象とするシステムを決定する。	(1) ロボットによるアクセスがルールやライセンスで制限されていないこと。 (2) アプリケーションレベルでのアクセスログや操作ログが取得可能であること。 (3) ロボットの誤処理やテスト処理で更新されたデータを特定し、修正するための機能が実装されていること。 (4) システムの変更により、ロボットが行う業務に重大な影響をおよぼす可能性がある場合は、当該システムの管理部門と連携し、事前に対応の検討が可能であること。
e-3	インフラ環境に対する要求事項	ロボットを実行する端末、開発する端末、ネットワーク等に求められる要件に適合したインフラ環境を整備する。	(1) ロボット端末やロボット管理サーバーには、社内の端末や情報システムと同様のシステム管理にかかわるルールやセキュリティにかかわるルールが適用されること。 (2) ロボット端末へのアクセスを物理的・論理的に制限するとともに、そのログをモニタリングすること。 (3) RPAツールを導入している端末を特定・把握し、ロボットの動作に影響を及ぼすような保守計画を把握する仕組みがあること。 (4) 処理件数増加や高速・大量通信への対応等、ロボット端末やネットワークのスケーラビリティが高いこと。

第3章　RPAガバナンスの構築方法

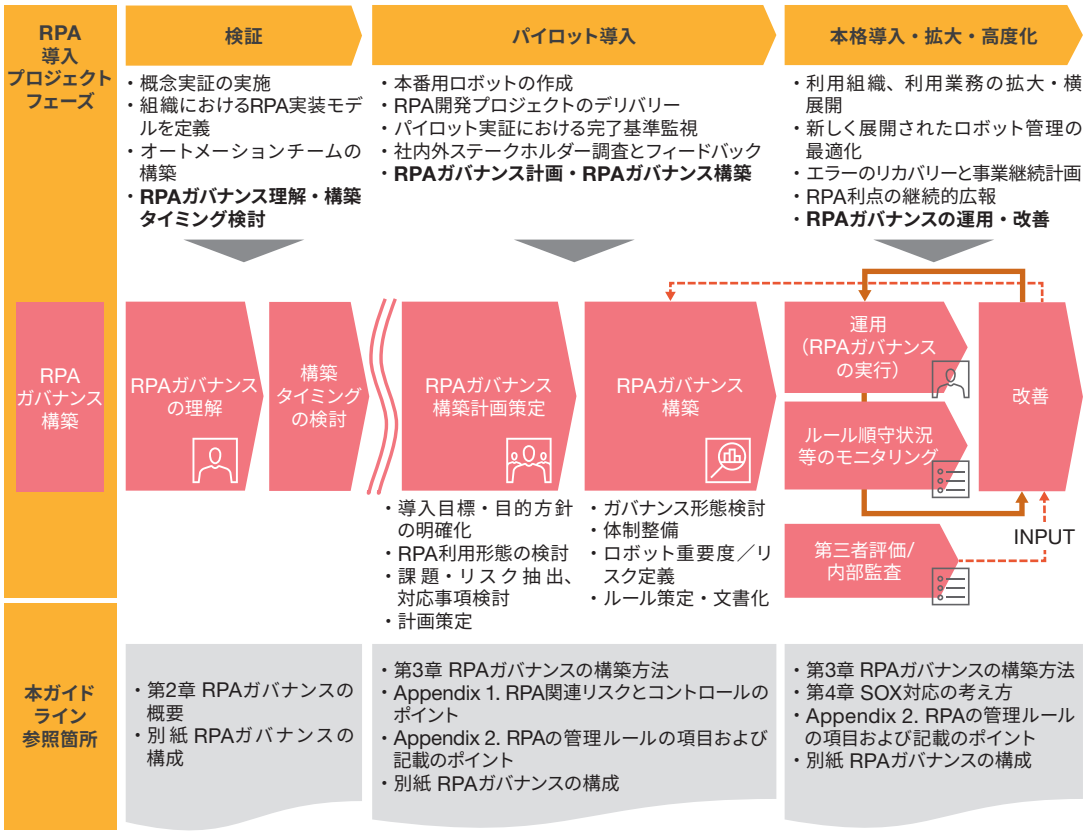
本章では、RPAガバナンスの一般的な構築方法について説明する。本章で説明する構築方法は、新規に構築する場合の例である。既に構築済の場合は、主に「(カ) ルール順守状況等のモニタリング」以降を参照いただきたい。

1. RPAガバナンスの構築と運用管理の全体像

各企業のRPA導入状況によって構築の目的は異なるものの、原則的に、RPAの本格導入時までには最低限のRPAガバナンスが構築されていることが望まれる。RPAを導入に伴い新規にRPAガバナンスを構築していく場合は、例えば概ね図9のような進め方になるものと考えられる。RPAガバナンス構築の各工程における詳細な内容は次項の「2.RPAガバナンス構築方法」を参照していただきたい。

なおRPAガバナンスは、一度構築して終わりではない。RPAガバナンスの運用はもちろんのこと、内外の環境変化に応じて求められる要件が変わるため、継続的な改善を行うことも重要であり、既存のガバナンスに課題があるなど、場合によっては再構築が必要となるケースもある。そのため、ここでは、RPAガバナンス構築後のモニタリングや評価、改善等といった取り組みも対象に含め説明する。

図9：RPAガバナンス新規構築のアプローチ（例）



2. RPAガバナンス構築方法

（ア）RPAガバナンスの理解

RPAガバナンスの構築においては、RPAガバナンスを理解することが大前提となる。第2章「3.RPAガバナンスの全体像」のとおり、RPAガバナンスは、「狭義のRPAガバナンス」とRPAマネジメントに大別されるが、多くの企業はRPAマネジメントのみ、その中でも管理ルールや開発標準の作成といった局所的な対応を取っているケースが多い。RPAガバナンス構築に向けて、どういった体制やルールを整備すべきなのか、PDCAサイクルを回すべきなのか、どのように経営者がかかわるべきなのかなど、RPAガバナンスを十分に理解することが望まれる。十分な理解が進めば、経営層を含む関与者に対し説明もしやすくなるであろう。

（イ）構築（再構築）タイミングの検討

これからRPAを導入するのであれば、当然のことながらルール等、何らかのガバナンスは必要となるが、有効性を検証するためのPoC[3]のような段階では、RPAガバナンスについて議論するのは時期尚早となる。

一方、本格導入のタイミングでの構築は、RPAの導入が進み、多数のロボットが開発・利用されつつある状況なので、急ぎ構築する必要がある。また何らかのガバナンスのもと既にRPA導入が進んでいるのであれば、場合によってはRPAガバナンスの再構築が必要となる。

そのため、RPAの導入状況を鑑みて、ガバナンスをどのタイミングで（いつからいつまでに）どの程度のレベルで構築し、展開・実行するのが最適であるのかを検討することが重要である。

これらを考慮すると、RPAガバナンス構築、または再構築を検討する場合、以下のどのようなタイミングに該当するか、検討することが望まれる。

＜RPAガバナンス構築のタイミング（例）＞

- 本格導入開始までに構築（パイロット終了までに構築）
- 本格導入を開始し、その状況を踏まえ、半年以内に構築

＜RPAガバナンス再構築のタイミング（例）＞

- 既に導入が進んでおり、各所でルール違反のようなものが散見されるため、SOX対象業務へのRPA適用開始までに再構築（SOXに対応したRPAガバナンスを構築）
- RPA利用方針変更に伴うRPA利用形態の変更により、利用形態の変更に合わせ再構築
- 既存の開発ルール等にのっとることを前提としていたが、RPA利用開始後にRPAの利用実態と合っていないことが判明したため再構築
- 外部監査人からの指摘への対応と合わせ再構築

3　PoCとは、「Proof of Concept」の略語であり、日本語では「概念実証」などと呼ばれ、新しい概念やアイディア、技術等について、実効性や実用性を検証するために行う試行などのことを指す。

（ウ）RPAガバナンス構築計画の策定

RPAガバナンスは、単なるルールの話ではない。RPA導入目標を安全に達成していくための仕組みであるため、当該目標・目的・方針の明確化や、その仕組みを運営していくための体制も必要である。当然のことながらルールも策定することとなるが、そのルールも実態に対して過剰なものであってはならず、また過小なものであってもならない。よってRPAガバナンス構築においては、計画策定がより重要となる。

その計画策定では、例えば以下のようなことを行うことが望まれる。

- RPA導入目標・目的・方針の明確化

  RPAガバナンス計画策定においては、まずは経営を交えて議論したうえで、RPA導入目標・目的・方針を明確化する必要がある。例えば、数年以内に何百万、何十万時間を削減する目標とするのであれば、大規模にRPAを導入していく必要があり、より組織的な取り組みや多くの人員にもルールを浸透させていく必要がある。一方で、そこまで大きな目標は掲げないものの、多くの社員がデジタルツールを扱えるようにするなどといったことを目的とするのであれば、求められる体制やルールも違ったものになるであろう。またRPA導入を進めるものの、会社レベルでの導入ではなく、本部レベルやIT施策の一環での導入といった割と小規模を対象とした導入方針の場合、大規模な体制やそれを想定したルールである必要はないであろう。

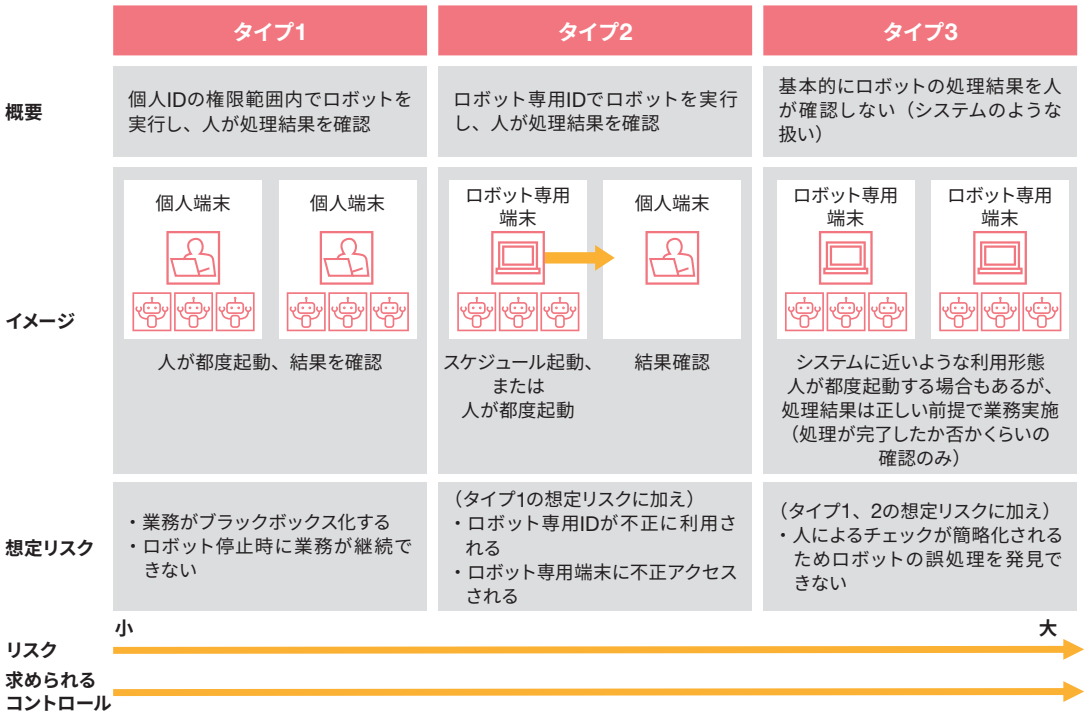
  このようにRPAガバナンスは、RPA導入目標・目的・方針によって求められるものが変わるため、当該目標・目的・方針を明確化することが、最初に必要である。

- RPAの利用形態の検討

第2章でも述べたとおり、RPAの利用形態によってリスクと求められるコントロールは異なる。例えば、以下の図10のタイプ1の場合、個人IDの範囲内で開発・利用することとなるので、表計算ソフトのマクロ機能と同じような使い方となる。RPA固有のリスクがあるので完全に同じものではなく、これまで各企業が直面したスプレッドシートの問題があるので慎重に進める必要はあるが、人がその都度起動するなど、マクロの延長としての利用に制限を加えることで、求められるルール等も簡易的なものとなるであろう。一方、タイプ2のようにロボット専用にIDを発行し、当該IDを利用してロボットが各システムにアクセスする場合はどうであろうか。例えば人が関与しなくてもロボットは処理を実行することが可能であるため、もはや人が都度起動するといったマクロの延長とは言えない。そうすると、ロボット専用に発行したIDの管理や、ロボット端末の物理的な管理等、求められるルールなどはより高いレベルが求められるだろう。続いてタイプ3を見ると、ロボットの処理結果が正しい前提で業務を行うなど、人の介在を極力省くことになるため、求められるルールはさらに高いレベルのものが必要になると考えられる。

このように、目指すべきRPAの利用形態がどのようなものであるか把握することも、RPAガバナンス構築においては必要となる。また、RPAの利用形態は、必ずしも段階的にいずれか一つの利用形態になるとは限らず、例えばタイプ1とタイプ2の利用形態を併用して利用する場合もある。また最初からタイプ3を目指す場合もあるため、各企業や組織のRPA導入方針や目的に適した利用形態を検討することが重要である。

図10：RPA利用形態のイメージ



- （既にRPA導入が進んでいる場合）RPA導入状況の実態把握

  既にRPA導入が進み、多くのロボットが稼働している場合、それらロボットを棚卸し、どういったロボットが稼働しているのか、RPA導入状況の実態を把握することも重要となる。前述のとおり、RPAの利用形態に応じて、構築するガバナンスのレベルは異なる。タイプ1を想定してガバナンスを構築しようと考えていても、タイプ2、タイプ3のような利用をしているロボットがあるのであれば、タイプ2、タイプ3を想定してガバナンスを構築せざるを得ないであろう。または、タイプ1の場合のルール、タイプ2、タイプ3の場合のルールなど、ルールを分けるようなガバナンスを構築することになるであろう。このように、RPA導入状況の実態に即したガバナンスを構築するために、RPA導入状況の実態把握を行うことが重要となる。

- ガバナンスレベルでの課題抽出、対応方針の検討

  第2章のRPAガバナンスの構成要素等を理解し、別紙「RPAガバナンスの構成」を活用すれば、ガバナンスを構築または再構築する際の現状の課題や阻害要因となりうる事項を把握できるであろう。抽出した課題は、現在のルールや体制を少し見直せば解決するものもあれば、抜本的に見直す、または新たに作る必要があるものもあるかもしれない。また経営者を交え協議しなければ解決しないものや、組織の見直しなど人事異動を伴うものが含まれる可能性もある。

  RPAガバナンス構築や再構築においては、ガバナンスレベルで抽出した課題に対し、短期的視点と中長期的視点の両面で対応方針を検討することが望まれる。中長期的に対応する課題については、暫定対応を検討した上で、継続的なモニタリングや改善の中で対応していくことが考えられる。

- 計画策定

  前述までの取り組みを通じて、RPAガバナンスの課題・リスクへの対応事項は洗い出されているため、スケジュールを組みながら具体的に計画にしていくこととなる。構築する内容によっては、例えば規程類であれば経営者の決裁が必要になる可能性が高い。また、体制であれば人事異動等を要するため、ある程度の余裕をもったスケジュールになるであろう。またSOX対応も踏まえたものを計画するのであれば、SOX文書の作成や外部監査人との調整等も必要となるため、スケジュールにはその点も踏まえておくことが望まれる。

（エ）RPAガバナンス構築

RPAガバナンス構築は、前述で説明した計画に基づき構築を進めていくこととなる。本項では、構築フェーズの代表的な取り組みについて説明する。

- RPAガバナンスの形態の検討

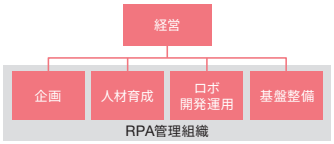
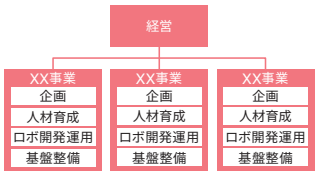
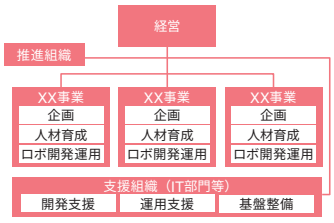
  RPAガバナンスの形態は「集権型」「分散型」「連邦型」の3つに大別される。どのような形態を目指すのか、大枠でそれぞれのメリット・デメリットを踏まえ、RPA推進体制の検討をしていく必要がある。

  ≫ **集権型**：全社的な戦略・方針に従いRPAを導入し、全社的な推進組織がRPAのツール基盤、開発・運用体制、管理ルールを整備・管理しているようなガバナンス形態

  ≫ **分散型**：各事業部門が個別にRPAツールを選定・導入し、維持・管理しているようなガバナンス形態

  ≫ **連邦型**：RPAの導入や利用は各事業部門の判断にて実施しているが、全社的な推進組織が管理ルールの策定・展開、RPAシステムの提供、開発支援など一程度関与しているようながバナンス形態

図11：RPAガバナンスの組織形態

	イメージ	特徴	メリット・デメリット
集権型		・RPAに関する施策はトップダウンで決定・展開 ・経営が各種取り組みをコントロール ・標準化された基盤、導入・運用プロセス	【メリット】 ・意思決定の迅速化、トップダウン ・標準化、全体最適 【デメリット】 ・事業部固有ニーズへの対応は遅れる
分散型		・事業部にあったRPAの導入・展開を実施 ・事業部の責任者が事業部のRPAの取り組みをコントロール ・IT部門やコンプライアンス部門等、関連部門との調整は必要	【メリット】 ・事業部固有ニーズへの対応の迅速化 【デメリット】 ・連携・調整不足の発生 ・コントロール水準の維持が困難（野良ロボが発生する可能性あり） ・ナレッジ共有が困難、高コスト化
連邦型		・RPA開発の予算自体は事業部が管理し、開発実施 ・IT部門等は、RPA支援組織として開発・運用、基盤整備支援を行う。 ・事業部と支援組織の役割分担の明確化は必要	【メリット】 ・集権型、分散型の両メリットを享受 ・推進組織による連携・調整 【デメリット】 ・推進組織、事業部、支援組織の役割分担の設計・変更が難しい

- 体制の構築

RPAガバナンスの形態、RPA利用形態に応じて、必要な組織、組織の役割は異なるものの、いわゆる3ディフェンスライン[4]の考え方も踏まえると、例えば以下のような役割を担う組織が必要となる。なお、それぞれが独立した組織となることもあれば、複数の組織の機能を1つの組織で担う場合（例えば、利用組織と開発組織が1つの組織になるケースや全社推進・管理組織と運用組織が1つの組織になるケース）もある。いずれの場合も、それぞれの組織の役割を参考にしつつ、自社の組織構成、役割・責任を検討し、最適な組織設計をすることが望まれる。

＜組織の役割・責任（例）＞

a. 全社推進・管理組織

経営者の方針のもと、RPA利用にかかわる全社的な目標や計画、ルールを定め、各利用組織のRPA導入状況や効果、ルール順守状況等を把握し、定期的に経営者へ報告する。また、RPAにかかわるナレッジや人材育成、管理手順の整備・提供等、利用組織がRPAを効果的かつ安全に利用するための支援施策を実施する。

b. 利用組織

ロボットを利用して業務を行い、ロボットを利用した業務の実行・品質について責任を負う。必要に応じて、開発組織と連携し、業務要件定義やロボットのテストを行う。

c. 開発組織

ロボット企画、開発、テストを行い、ロボットの品質について責任を負う。

d. 運用組織

RPAシステムの運用管理およびロボットの運用監視を行い、RPAシステムのリソース管理やセキュリティについて責任を負う。

e. リスク管理組織

RPAの利用に当たり、セキュリティやロボットのリスクの審査を行う。改善が必要なロボットについては、開発組織と連携し、リスク低減に必要な措置を講じる。RPAとは別の社内組織の場合もあるため、RPAガバナンス構築前に、全社推進・管理組織と連携し、RPAに関して理解を深めることが望まれる。

f. 内部監査組織

利用組織がRPAを利用して行う業務について、内部統制評価などの内部監査を行う。監査内容にRPAの処理内容が関係することも少なくないため、RPAに関して理解を深めることが望まれる。

4　3ディフェンスラインとは、リスクオーナーとしてリスクコントロールを行う第一のディフェンスライン、リスクに対する監視を行う第二のディフェンスライン、リスク管理機能および内部統制システムに対し合理的な保証を提供する第三のディフェンスラインの3つのディフェンスラインに分け、リスクマネージメントと組織のコントロールを機能させる体制の考え方を指します。

- ロボットの重要度／リスク度合いの定義

RPAは便利ツールのようなものから、システムと同等の処理を行うものまで多様だ。言い換えると、業務への影響度合いにより重点的に管理すべきものとそうでないものに分けられる。よって重点的に管理すべきロボットを特定できるよう、ロボットの重要度・リスク度合いの考え方を定義しておくことが重要である。例えば、図12のように機密性、完全性、可用性の各観点でリスクを「高」、「中」、「低」等の3段階に分類して評価を実施し、それらの評価をインプットにロボットの重要度・リスク度合いを「最重要」、「重要」、「一般」等、レベル分けを行い管理することが望まれる。

図12：機密性、完全性、可用性の定義（例）

	機密性	完全性	可用性
高	個人情報等、漏洩した場合、**対外的な影響を及ぼす**ような情報を取り扱っているロボット。	誤入力・誤処理した場合、**対外的な影響を及ぼす**ような処理を行っているロボット。	処理が停止した場合、代替がきかず、**対外的な影響を及ぼす**ようなロボット。
中	漏洩してた場合、業務に重大な影響を及ぼすものの、**対外的な影響までは及ぼさない**情報を取り扱っているロボット。	誤入力・誤処理すると、業務に重大な影響を及ぼすが、**対外的な影響までは及ぼさない**処理を行っているロボット。	処理が停止した場合、代替がきかず、業務に重大な影響を及ぼすが、**対外的な影響までは及ぼさない**ロボット。
低	「高」「中」に当てはまらないロボット。	「高」「中」に当てはまらないロボット。	「高」「中」に当てはまらない。

機密性、完全性、可用性の観点での評価をベースに
「最重要」「重要」「一般」等、
ロボットの重要度（リスク度合い）のレベルを定義

- ルール策定

RPAにかかわるルールの策定において、まず行うべきはルール体系および優先度の検討である。

ルールの階層はおおむね3階層あり、経営層が定める方針、管理者層が定める規程・基準、現場層が定める手続きがある。経営層のRPA導入、利用に関する基本的な考えや方針を反映したものをRPA基本方針といい、前述の全社推進・管理組織が方針に沿って制定するものをRPA管理規程や基準、それらの管理ルールに従い作成するものをいう（以下総称して「RPA管理ルール」と表記する）。

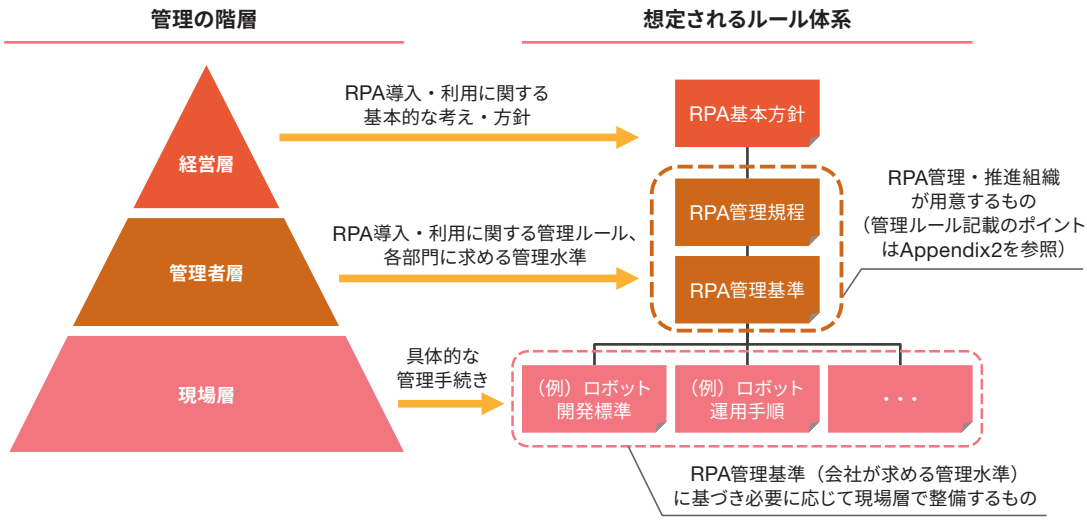
これらのルールはRPAについて独立したルールとして新たに策定することもあれば、既に規定されている情報システム等のルールに従うこともある。既存の情報システム等をアップデートし、不足する内容を追加する方法もある。これらを踏まえ、自社の状況や組織の形態等に応じて、適切なルール体系を検討することが望ましい。なお、全社推進・管理組織が制定すべきRPA管理規程・基準の例としてAppendix2に規定・基準レベルの項目および記載ポイント例を記載しているので、そちらを参考にすることが望まれる。

また、SOX対象業務にRPAを適用する場合または適用を検討している場合は、第4章「SOX対応の考え方」を参照していただきたい。

RPA管理ルールは、RPAの利用状況等に応じて、どのルールを優先的に整備するかを検討する必要がある。RPA利用が一部の部署等にとどまる場合には、方針、規程・基準まで正式に整備し、詳細な手順は事後的に整備することも可能であろう。また、方針、規程・基準を整備した上で、一部の重要な手続きのみ整備し、その他の手続きは事後的に整備することも可能である。どのルールを優先的に整備すべきか、は整備にかかわる時間とRPA利用の進展状況により変わるため、自社の状況を見極めた上で必要なルール体系、優先度を検討することが望ましい。

また、それぞれのルールの内容についても、RPAの利用が拡大するにつれて、より厳格なものが要求されることが一般的であり、社会情勢、法令の対応や技術の発展等、社内外の状況により、ルールをアップデートしていくことが望まれる。このため、RPA管理ルール（特にRPA管理規程、RPA管理基準）を策定したら不可侵のものとして扱うのではなく、定期的にメンテナンスや変更の検討を行うことが求められる。

図13：ルール体系の例



（オ）運用（RPAガバナンスの実行）

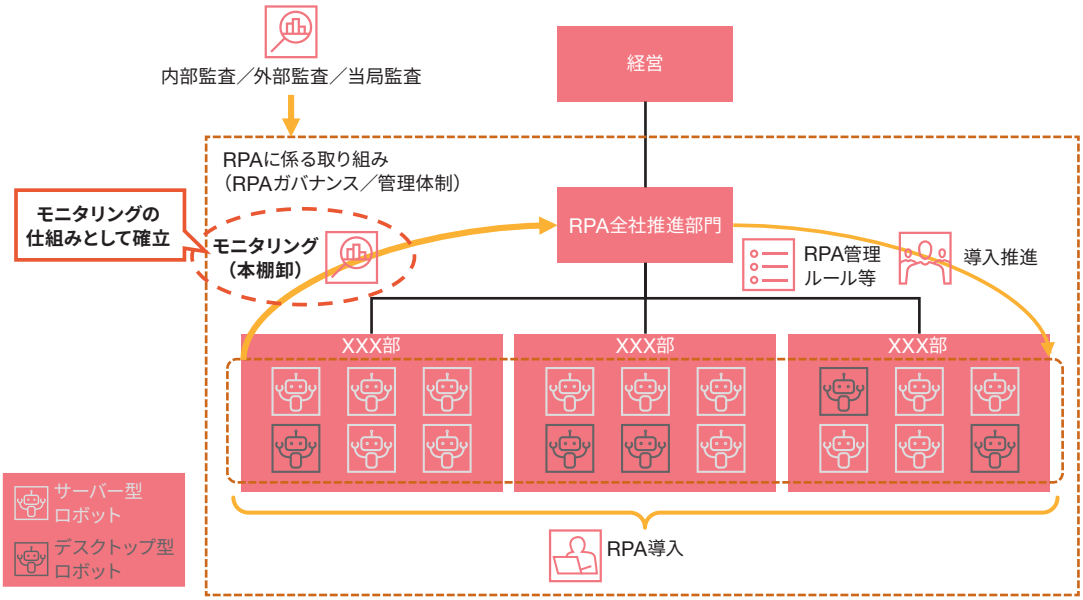
各RPA関連組織は、策定されたRPA管理ルールに従い、RPAを利用することが望まれる。全社推進・管理組織は、各組織がルールどおり運用できるよう、サポート窓口等を開設し、各組織のサポートを提供することが望ましい。

（カ）ルール順守状況等のモニタリング

RPAは、過度なガバナンスだと導入が進まないため、ある一定程度の“緩さ”を持たせることも必要となる。しかしながら“緩い”だけではリスクが高くなる一方であることから、ルール順守状況をモニタリングし、不備等が識別されたら是正させていく仕組みが必要となる。

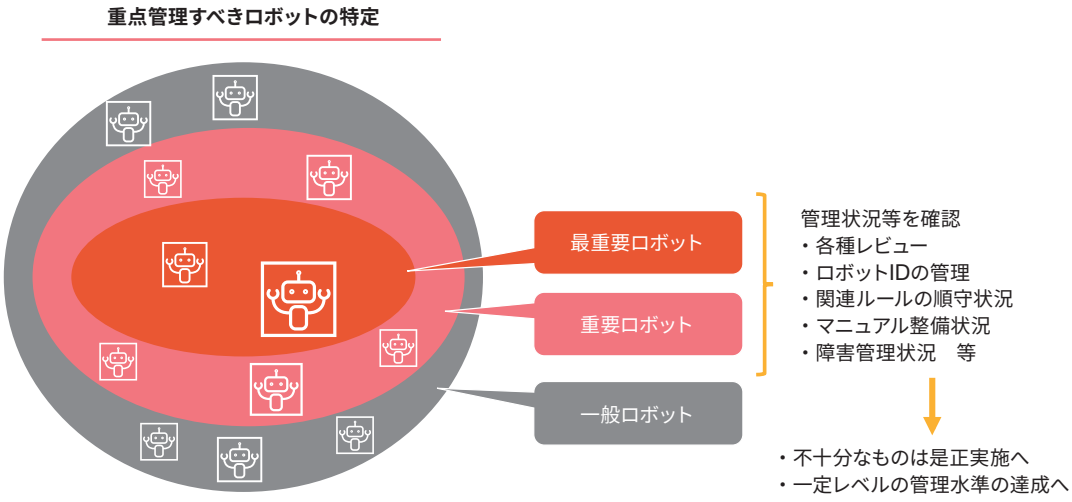
また、RPAの利用形態が変わった場合、例えばタイプ1からタイプ2へ変更となった場合、利用形態が変わるため求められるコントロールのレベルは一般的には高くなる。そのような場合もロボットの重要度やリスクに変更がないか、新たにリスク評価を行う必要があり、それらの評価のインプットをもとに改善を行うことが望ましい。

図14：モニタリングのイメージ



なおモニタリングは、全てのロボットを対象とするのではなく、効率性の観点から必要に応じて前述の重要度／リスク度合いの評価で「最重要」「重要」等と位置付けたロボットを優先して実施するといった方法（いわゆるリスクアプローチ）が望まれる。重要度／リスク度合いの高いロボットについては各種レビューを強化するなど、重点的に管理することが望まれる。

図15：重要度／リスク度合いの高いロボットの管理イメージ



（キ）第三者評価／内部監査

RPAガバナンスの有効性を評価するためには、内部監査や第三者評価（外部監査）を定期的に受ける必要がある。第三者による客観的な評価を行うことで、RPAガバナンスを構築し、実行している当事者では気付かないようなリスクを把握し、そのリスクが顕在化する前に対処することが可能となる。

（ク）改善

RPAガバナンスは、一度構築して終わりではない。内外の環境変化によって課題が生じたり、リスクが増減したりするため、継続的な改善が必要である。よって定期的にRPAガバナンスを見直し、必要に応じて改善を図っていくことが望まれる。その際、前述のモニタリングや第三者評価／内部監査の結果をインプットとして活用することは、有効な取り組みであると考えられる。

第4章　SOX対応の考え方

本章では、金融商品取引法の財務報告に係る内部統制報告制度（通称「J-SOX」）が適用される日本の証券取引所に上場している企業や、米国のサーベンス・オックスリー法（通称「US-SOX」）が適用される企業において、RPAを導入する場合の対応について説明する。

J-SOXとUS-SOX（以下、両者を合わせてSOXと表記）は、スコープや外部監査人による監査の内容等は異なるが、いずれも財務報告に係る内部統制の構築が義務付けられている。そのため、SOX対象企業は、RPA適用対象業務によっては、当該内部統制に影響を及ぼす可能性があるため、何らかの対応が要求される。なお、ここでは内部統制の構築までの説明とし、SOXで求められる経営者評価等については割愛する。

また、SOXについての基礎的な説明は本章「4. SOXの基礎知識」にて補足しているため、必要に応じて参照していただきたい。

1. RPAとSOXの関係性

- RPAとSOXの関係

  財務報告に係る内部統制は、経理・主計業務だけの話ではなく、受注入力を行う営業部門や発注業務を行う購買部門等、企業のさまざまな部門が行っている業務も対象となる。また上場企業であれば、SOX対応が義務化されている。このため、RPA適用対象業務によっては、RPA導入時に何らかのSOX対応、すなわち財務報告に係る内部統制の構築が必要となる。またその対応が不十分であると、外部監査人から指摘を受けるばかりか、場合によっては“内部統制に欠陥がある”といった監査意見が出される可能性がある。なお、第2章で対応が不十分な場合に生じる影響を記載しているため、適宜参照していただきたい。

- SOX対象業務へのRPA適用は禁止すべきというのは誤った解釈

  SOX対象業務へのRPA適用は行ってはならないという考え方もあるが、それは誤った解釈だと考えられる。内部統制への影響を考慮しながらRPAを適用すれば、SOX対応は行えると考えられる。次節ではRPA導入におけるSOX対応のポイントについて説明する。

2. RPA導入におけるSOX対応の基本的な考え方

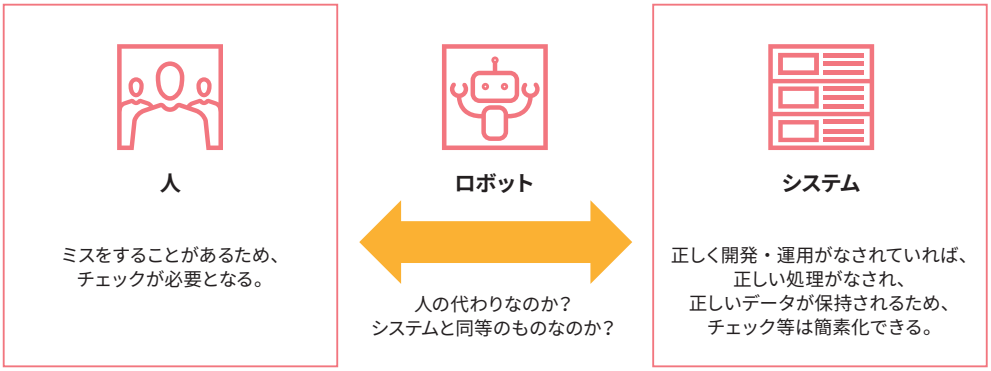
- 基本的な考え方

これまでSOX対応において何ら問題がなかったのに、なぜRPAを導入すると何らかの対応が求められるのであろうかと、多くの方が疑問を感じるかもしれない。その根本は、ロボットは人の代わりなのか、システムと同等のものなのかという考えに基づくものであろうと思われる。

例えば、ロボットを人の代わりとして扱うのであれば、「人と同じようにミスをする」という前提のもと、ロボットの処理結果を、従来どおり人がチェックする。そのため、処理結果に誤りがあったとしても、それを発見できるであろう。しかし、「システムと同様、ロボットの処理結果は常に正しい」として扱うならば、処理結果が正しい前提で業務を進めることとなるため、誤りがあったとしてもそれを発見できないであろう。

このことは、ロボットをシステムと同様に扱ってはならないというものではない。そのような対応を行う場合、ロボットが行う処理の信頼性をいかに担保するかが重要となることを指している。

図16：ロボットの位置付け検討イメージ



≫ 人の代わり：ロボットは人と同じようにミスをする。
≫ システムの代わり：システムと同じように、ロボットの処理結果は常に正しい。

では、これらを財務報告に係る内部統制に置き換えたらどうであろうか。

例えば、“担当者が照合して、その結果を管理者が確認する”という統制を考えてみよう。“担当者が照合する”部分をロボットが行い、“結果を管理者が確認する”部分を従来どおり管理者が行うのであれば、ロボットによる誤処理等は発見できる可能性がある。一方で、ロボットが行う処理は常に正しい、として扱い、“結果を管理者が確認する”部分を割愛したらどうなるであろうか。ロボットに誤処理等があった時、それを発見できず、結果として不整合なデータに基づき会計処理等が行われてしまう。このため、ロボットをシステムと同様に扱って業務を行う場合、当該ロボットの処理は正しいのか、そして当該ロボットが正しく開発され、運用プロセスの整備やモニタリング、データ保護がなされているかなども重要となってくる。

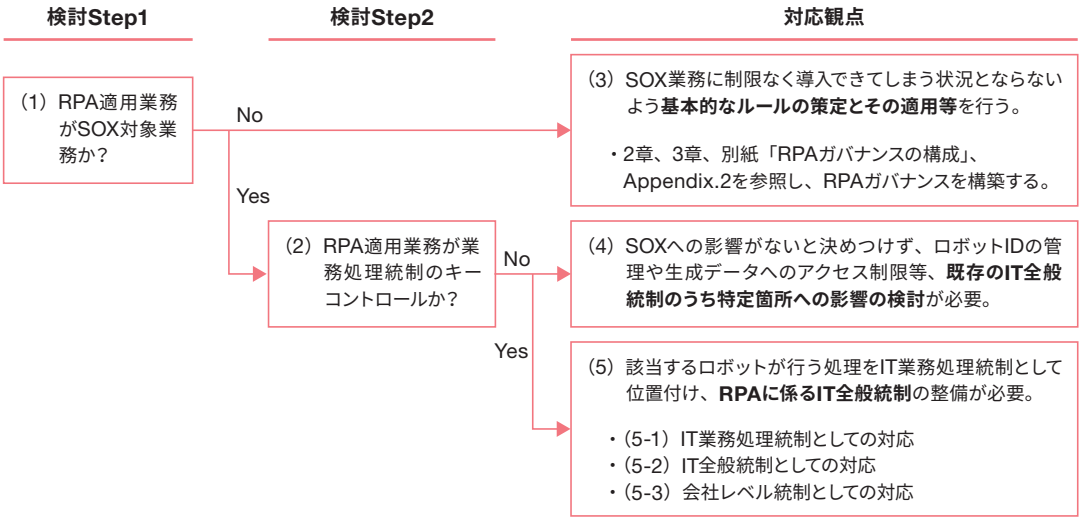
また、RPAの利用に当たっては、ロボットは1体だけでなく、場合によっては何百体と利用されていることもあり、それぞれのロボットで、利用の前提となる考え方が異なる可能性があるため、会社としてのRPA管理ルールや体制等も重要になってくる。

3. RPAにおけるSOX対応の観点

具体的にどのようなSOX対応を行う必要があるか、SOX対象業務へRPAを導入する場合のポイントを説明する。RPAにおけるSOX対応は、例えば以下のフローに沿って検討することが望まれる。

なお以下のフローはあくまで例であり、実際は自社のSOX担当部門や外部監査人と協議し、進める必要がある。またそのような協議がSOX対応の一番の成功要因となる場合がある。

図17：SOX対応検討フロー（例）



（1）RPA適用業務がSOX対象業務かどうかの確認

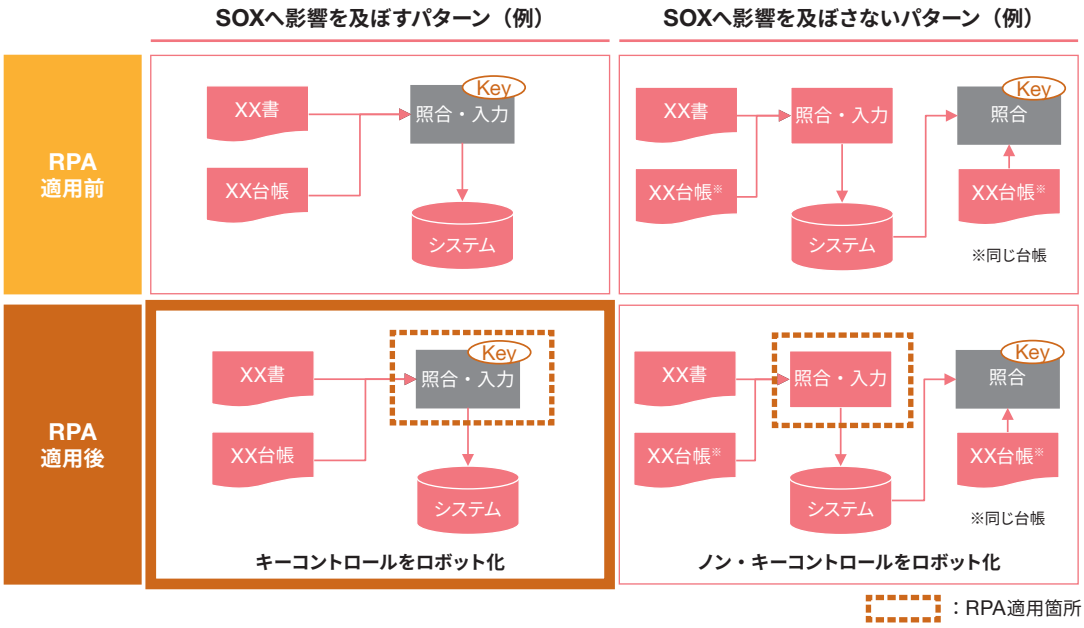
まず確認すべきは、RPAを適用する業務がSOX対象業務か否かである。SOX対象企業では、通常SOX対象業務が明確にされているため、RPA適用業務がSOX対象業務か否かを確認することが可能である。

ただし、US-SOX対象企業の場合は、SOX対象業務が年ごとに変わる可能性があることを考慮する必要がある。US-SOXとJ-SOXでは、重要な勘定科目の決定方法が異なる。US-SOXは、税前利益の5%等、金額から重要な勘定科目が決まり、そこからSOX対象業務が決まる。一方でJ-SOXは、既に重要な勘定科目が決まっており、それを構成する業務プロセス等からSOX対象業務が決まる。よって、US-SOX対象企業の場合、業績の変動によって、SOX対象業務が年ごとに変わる可能性がある。このため、US-SOX対象企業は、RPA導入当初から、SOX対応を見据えてRPAガバナンスの構築を行うことが必要である。

(2) キーコントロールにRPAを利用しているかの確認

次にRPA適用業務がSOX対象業務であっても、ノン・キーコントロールの業務処理にのみRPAを利用する場合、SOXへの影響がないことも考えられる。SOX対象企業であれば、業務処理統制のSOX文書として3点セット（業務フロー図、業務記述書、リスク・コントロール・マトリックス）が作成されており、その中でキーコントロールも明確化されているであろう。このキーコントロールがロボットに置き換わるのかなど、RPAが業務処理統制のキーコントロールに影響を及ぼすか否かを確認する必要がある。

図18：SOXに影響を及ぼすパターン（例）



(3) SOX対象業務以外の業務のみにRPAを適用する場合の対応の考え方

SOX対象業務以外の業務のみにRPAを適用する場合、知らない間にSOX対象業務へRPAを導入されないように管理することが必要である。例えば、ロボットの開発・変更に関するルールを整備し順守させる、開発者と利用者の職務を分離する、RPAを導入した時点ではSOX対象ではなかったとしても、ロボットの適用範囲変更や拡大により、SOX対象業務へ適用されてしまうといった可能性があるため、ロボットの利用状況を定期的に確認するなどが考えられる。

なお、そもそもSOX対象業務へのRPA適用を禁止している場合でも、知らない間にSOX対象業務へRPAを導入されないようルールを整備し管理することが必要である。

また、ロボットが各システムにアクセスできるようにロボット専用IDを発行している場合は、SOX対象業務のシステムを知らぬ間に利用されないよう各システムにおけるロボット専用IDの管理ルールを整備し、管理する必要がある。

(4) ノン・キーコントロールの業務処理のみにRPAを利用する場合の対応の考え方

ノン・キーコントロールの業務処理のみにRPAを利用する場合でもSOX対象に影響はないと決めつけてしまうにはまだ早い。業務処理のキーコントロールに影響がない使い方をしていても注意すべきことがある。例えば、ロボットが各システムにアクセスできるよう、ロボット専用IDを発行しているような場合、当該ロボット専用IDの不正利用に対する統制等、既存のIT全般統制に対する影響の検討が必要となる。

もしも経費入力ロボットに経費システムへアクセス可能なIDを発行し、それを役席者が管理する場合、役席者が当該ロボット専用IDで経費入力を行い、その後、自身のIDで経費承認を行うといった自己入力・自己承認ができてしまう。また、ロボットの生成したデータが、誰でもアクセスできる場所に保管されている場合、当該データの改ざんもできてしまう。これらの状況にある場合、リスクが十分に低減できているとはいえないため、外部監査人から指摘を受ける可能性がある。

(5) キーコントロールの業務処理にRPAを利用する場合の対応の考え方

キーコントロールの業務処理にRPAを利用する場合、「(5-1) IT業務処理統制としての対応」、「(5-2) IT全般統制としての対応」および「(5-3) 会社レベル統制としての対応」の対応が必要となる。

また、RPAの管理ルールにおいてAppendix2に規定・基準レベルの項目および記載ポイント例を記載しているので、そちらの利用形態「タイプ3」の記載ポイントを参考にすることが望まれる。

(5-1) IT業務処理統制としての対応

業務処理統制とは、業務プロセス中に存在する統制を指す。さらに業務処理統制は、ユーザーがマニュアルで行う「マニュアル統制」とITアプリケーションの機能によって実行される「IT業務処理統制」がある。なお、ITアプリケーションで実行される統制については、その判断結果を人間が確認し、対処していることが多い。このようにITアプリケーションで実行される統制に依存するようなマニュアル統制を「IT依存統制」という。

RPAの利用においては、インプットとアウトプットが一致することを論理的に説明できるようにすることが必要である。業務処理統制のキーコントロールをロボットに置き換える場合、ロボットの行う処理が“正確”かつ“網羅的”に行われることを説明する必要がある。また、“正確”かつ“網羅的”であることを、SOX文書 (3点セット) やロボットの仕様書だけでなく、経営者による評価や外部監査にも対応できるよう、証跡 (取引記録等) の確保を行うことが必要になる。

＜確認観点＞

≫ 承認された取引のみ会計計上するためのエラーチェックをロボットが行う場合

- エラーチェックが“正確”であること。
- エラーチェックの対象取引が大量でも、全件を“網羅的”に処理すること。
- 上記2点をSOX文書 (3点セット) やロボットの仕様書だけでなく、経営者による評価や外部監査にも対応できるよう、証跡 (取引記録等) の確保を行うこと。

なお、ロボットの処理には単純なものから複雑なものまでさまざまなものがあると考えられる。単純なもの (例えば、エラーチェックがある値同士を照合するだけ) であれば、間違いが発生する可能性は高くないであろう。しかしながら、複数条件に照らして照合するもの (例えば、一定の金額未満または一定の金額以上を照合する) は間違える可能性が高くなるため、慎重に対応する必要がある。

また、ロボットの処理の正確性に加え、ロボットが生成するデータの保護も必要となる。例えば、ロボットが生成したデータが誰でもアクセスできる場所に保管されている場合、当該データを改ざんされ、正しくないデータが後続の業務処理に使用される恐れがある。ロボットが生成する中間データや処理結果のデータは、適切にアクセス権が設定されたシステムやフォルダで管理する必要がある。

(5-2) IT全般統制としての対応

ロボットが行う処理がITアプリケーション統制として位置付けられる場合、RPAにかかわるIT全般統制も必要となる。この対応は、既存のIT全般統制で対応するという方法もあるが、多くは既存のIT関連ルールとは別にRPAのルールが存在している、またRPA固有のリスクもあるため、最低でも既存のIT関連ルールとRPAのルールの差分となる部分については、別途RPAとしてのIT全般統制が必要となるであろう。なおRPAにかかわるIT全般統制の整備に当たっては、Appendix1にRPAにかかわるリスクとコントロールの考え方の例を記載しているので、そちらを参考にしていただきたい。

その他、近年ではロボット管理サーバーやロボット端末をクラウド上に配置している場合がある。もしIT全般統制の対象となるロボット管理サーバー、ロボット端末がクラウド上に配置されているのであれば、当該クラウド自体もSOX対象となるため、当該クラウドサービスの利用に当たっての自社（受託元）のIT全般統制、プロバイダー側（受託先）のIT全般統制の整備、運用、評価を行うことが求められる。なおプロバイダー側のIT全般統制は、受託元が評価することは困難な場合が多い。このため、受託先が取得している86号報告書[5]やSSAE18[6]等といった第三者保証報告書の活用も検討することが望まれる。またクラウド利用においては、そのような第三者保証報告書を取得しているか確認することが望まれる。

(5-3) 会社レベル統制としての対応

前述のITアプリケーション統制としての対応やIT全般統制としての対応は、個々のロボットに対する対応ではない。ある特定の部門だけ対応できていて、その他の部門は対応できていないという状況は好ましくない。そのため、会社として統制を担保できるよう、ルール整備やその順守のための取り組み、順守状況のモニタリング、ルールの継続的改善等といった、会社レベル統制としての対応も必要となる。これらは、2章、3章で記載したRPAガバナンスの構築によって対応できるであろう。なお、業務処理統制のキーコントロールに影響を及ぼすロボットがなかったとしても、上場企業等、SOX対象企業は、会社レベル統制としての対応が必要になると考えられる。

例えば、キーコントロールに影響を及ぼすロボットがないということは、“ロボットの処理結果は人がチェックする”というルールが存在していると考えられる。このように、SOX対象企業は、RPAにかかわる基本的なルール等、会社レベル統制の整備を行う必要があると考えられる。

5　86号報告書とは、日本公認会計士協会（JICPA）の監査・保証実務委員会実務指針第86号「受託業務に係わる内部統制の保証報告書」に基づき、受託会社監査人が提供する保証業務である。

6　SSAE18とは、「Statement on Standards for Attestation Engagements No.18」の略語で、米国公認会計士協会が定めた受託業務（各種アウトソーシングサービス等）を行う会社の内部統制の有効性を評価する保証基準である。

4. SOXの基礎知識

ここでは、上記で触れなかったSOXの基礎知識を説明する。なお、ここで説明するのはあくまで概要のため、より詳細を理解したい場合は、SOXの専門書籍等を熟読することを推奨する。

- SOXとは何か

  まず、SOXとは何であろうか。東京証券取引所等、日本の証券取引所に上場している企業は、金融商品取引法の財務報告に係る内部統制報告制度（通称「J-SOX」）が適用される。また、大手企業には、米国のニューヨーク証券取引所への上場等、SEC登録企業があるが、その場合サーベンス・オックスリー法（通称「US-SOX」）が適用される。

  J-SOX、US-SOXはスコープや外部監査の位置付け等が異なるため、別のものであるが、両者には“財務報告に係る内部統制の構築”、“経営者による評価”、“内部統制報告書の開示”、“外部監査人による監査”という共通点があり、その対応を各企業に求めている。このため、東京証券取引所等、日本の証券取引所への上場企業や米国証券取引委員会（SEC）登録企業は、SOX対応を行う必要がある。

- 「リスク」「内部統制」とは

  「財務報告に係る内部統制」の概要説明を行う前に、前提となる「リスク」や「内部統制」の考え方を説明する。

  例えば、“9時までに出社する”という目標があったとする。しかし“渋滞などでバスや電車が遅延し、9時までに出社できない”という事態となる場合がある。また“急な用事が発生し出社できない（または午前半休を取り9時に出社できない）”ということもあり得る。このように、“9時に出社する”という目標と乖離（かいり）する可能性がいわゆる「リスク」である。

  この「リスク」を低減するための活動のことを「内部統制」という。前述の“渋滞や事故等でバスや電車が遅延し、9時までに出社できない”というリスクであれば、“万一を想定し早くに家を出る”、“運行状況を適時に確認し代替ルートを利用する”というのが「内部統制」となるであろう。“急病となり出社できない”というのであれば、“病気にならないよう日頃から健康に気を付ける”といったことが「内部統制」となるであろう。

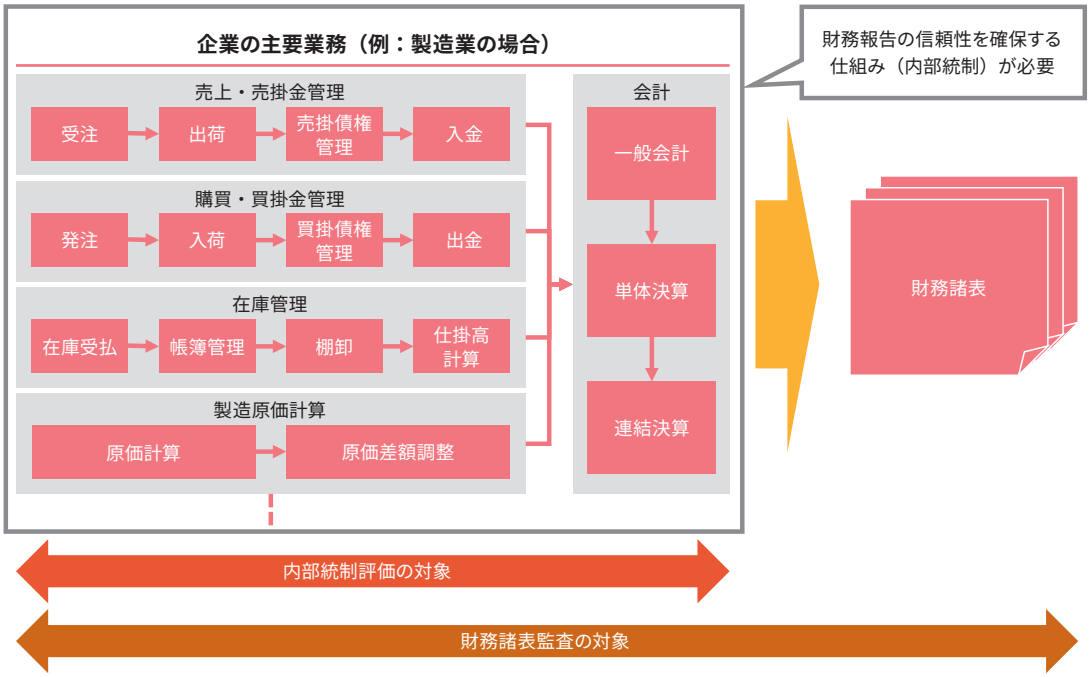
- 「財務報告に係わる内部統制」「キーコントロール」とは

「財務報告に係わる内部統制」とは何であろうか。まず、「内部統制」にかかわる「リスク」から考えてみることにする。

例えば、“誤発注を行い損失が発生する”といった事象を考えてみよう。一般的に“損失”というのは、企業の財務目標に影響を及ぼすため、「リスク」である。また“損失”とならないよう、“事業を見直す”というのは当該「リスク」に対する「内部統制」となるであろう。しかしながら、この例で示す「内部統制」は「事業活動に係わる内部統制」であり、「財務報告に係わる内部統制」ではない。「財務報告に係わる内部統制」が対象とするのは、あくまで「財務報告」であるため、前述の例であれば、“損失が正しく計上されない＝財務諸表が正しく作成されない”などといったことが「リスク」となり、それを低減する活動、すなわち“財務報告の信頼性を確保する仕組み”（不正または誤った財務報告を防ぐ仕組み）が、「財務報告に係わる内部統制」となる。また、その「財務報告に係わる内部統制」のうち最も重要な（効果的な）内部統制を「キーコントロール」と呼ぶ。

なお「財務報告」という言葉を見ると、財務諸表作成等を担う経理・主計業務の話と考える方もいるであろう。財務諸表は、企業の各部門の業務の集大成であるため、その財務報告は、経理・主計業務だけの話ではない。受注入力を行う営業部門や発注業務を行う購買部門等、企業のさまざまな部門が行っている業務も対象となる。また業務も、業務プロセスという視点で見ると、人が行う部分だけでなく、システム上で行われる処理もあり、これらシステム上で行われる処理も対象となりうる。またそのシステム上で行われる処理を深く考えると、処理を構成するプログラムやデータの信頼性も対象となる。

図19：財務諸表に係わる内部統制評価対象のイメージ



- 「会社レベル統制」「業務処理統制（マニュアル統制／ITアプリケーション統制）」「IT全般統制」とは

一般的に、財務報告に係わる内部統制として、以下の統制を整備・運用することが求められる。

① 会社レベル統制

組織全体における適切な統制の存在に関する保証を提供するために、経営者が保持している統制を指す。例えば、規程等といった経営者が社員に対して順守を求めているルールの存在や、当該ルールを順守させるための仕組み、順守状況のモニタリング、当該ルールの継続的改善等が該当する。

② 業務処理統制

業務処理統制は、業務プロセス中に存在する統制を指す。さらに業務処理統制は、ユーザーがマニュアルで行う「マニュアル統制」とITアプリケーションの機能によって実行される「IT統制」がある。なお、ITアプリケーションで実行される統制については、その判断結果を人間が確認し、対処していることが多い。このようにITアプリケーションで実行される統制に依存するようなマニュアル統制を「IT依存統制」という。

③ IT全般統制

ITアプリケーション統制が実行されているITシステムおよびその基盤を、継続的かつ有効に運用するための統制を指す。財務報告に関係しうるIT全般統制は、例えば以下の領域に分けられる。

＜4つのドメイン＞

- プログラム開発（要件定義、テスト等）
- プログラム変更（リリース、バージョン管理等）
- コンピューターオペレーション（バッチ処理、オペレーション管理、障害管理等）
- アクセス制限（ユーザー IDの登録・変更・削除・棚卸、パスワード管理、ログモニタリグ等）

さいごに

RPAの導入が日本で本格的に始まり、数年が経過しました。早いタイミングで導入し始めた企業は、既に1000体以上のロボットを稼働させ、何十万時間、何百万時間もの時間削減効果を得ています。その一方で、以下のような状況となり本格導入に至らないまたは全社展開が進まない場合や、効果が限定的になってしまうなど、RPAによる時間削減効果を得る機会を得られていない企業はまだまだ多い状況です。

＜本格導入に至らないまたは進まない原因例＞

- 経営者の理解を得られず、本格導入の意思決定がなされない、会社としてのRPA導入目標・目的が明確化されない
- 人材確保が厳しくなっていることは明確であるにも関わらず、目先のROI[7]にこだわり、RPA導入が進まない
- 自動化による時間削減といった分かりやすい効果だけに目が行き、品質向上や基幹システムの保守性向上、ロボットを用いたAI活用に向けたデータ整備等といった効果まで目が行かない
- RPAに対して漠然としたリスクを感じ、本格導入の意思決定を行えない
- ボトムアップでの推進によってロボットは増えたが、「プロセスの自動化」という考えが浸透しないためか、どれも便利ツールの域から脱せられず、結果として効果の高いロボットの導入が進まない
- 当り障りのないノン・コア業務のみを対象とした導入方針となっており、大きな効果が望まれるコア業務への導入まで行うような方針に至ってない
- 小さく始めて大きく育てるはずが、小さい状態のままである
- 人や組織の再配置に至らない

これらを見ると、前述のRPAガバナンスの構成要素の「戦略」部分に該当するもの、つまり多くの場合は「戦略」部分の欠如によってこのような状況になっているのではないかと考えられます。

本ガイドラインが述べているRPAガバナンスは、「RPA導入目標・目的を安心して達成していくための仕組み」という“攻め”と“守り”の視点が融合されたものであり、決して「安心して利用する仕組み」という“守り”の視点だけのものではありません。RPAガバナンスは、「RPA導入目標・目的を達成していく仕組み」という“攻め”の部分も重要であり、構成要素の「戦略」部分は大前提になります。

よって、RPAについて経営者を巻き込んだ議論・検討を通し、真のRPAガバナンスを確立、本格導入を加速させ、また他のデジタルテクノロジーとの連携等も進め、人や労働に関する経営課題の解決につなげて頂ければと思います。

多くの企業・組織がこの様な真のRPAガバナンス構築に取り組み、大きなRPA導入効果を得ることによって、ひいては日本の人や労働に関する社会問題の解決につながればと考えております。

7　ROIとは、「Return On Investment」の略語であり、投資利益率のことを指す。

【執筆者】

＜PwCあらた有限責任監査法人＞

宮村 和谷
システム・プロセス・アシュアランス部　パートナー

米山 喜章
システム・プロセス・アシュアランス部　シニアマネージャー

木本 達也
システム・プロセス・アシュアランス部　シニアアソシエイト

木戸 大嗣
システム・プロセス・アシュアランス部　シニアアソシエイト

望月 拓弥
システム・プロセス・アシュアランス部　シニアアソシエイト

＜UiPath株式会社＞

ビジネスコンサルティング室

【主な協力者】

＜PwCあらた有限責任監査法人＞

綾部 泰二
システム・プロセス・アシュアランス部　パートナー

平岩 久人
システム・プロセス・アシュアランス部　ディレクター

熊坂 翔太朗
システム・プロセス・アシュアランス部　アソシエイト

南木 春佳
システム・プロセス・アシュアランス部　アソシエイト

前田 翠
システム・プロセス・アシュアランス部　アソシエイト

【お問い合わせ先】

PwCあらた有限責任監査法人
RPAガバナンス担当
jp_aarata_rpa_gov@pwc.com

UiPath株式会社
ビジネスコンサルティング室
jp-bco@uipath.com

© 2019 PricewaterhouseCoopers Aarata LLC. All rights reserved.
PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2019 UiPath Inc., UiPath SRL

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.